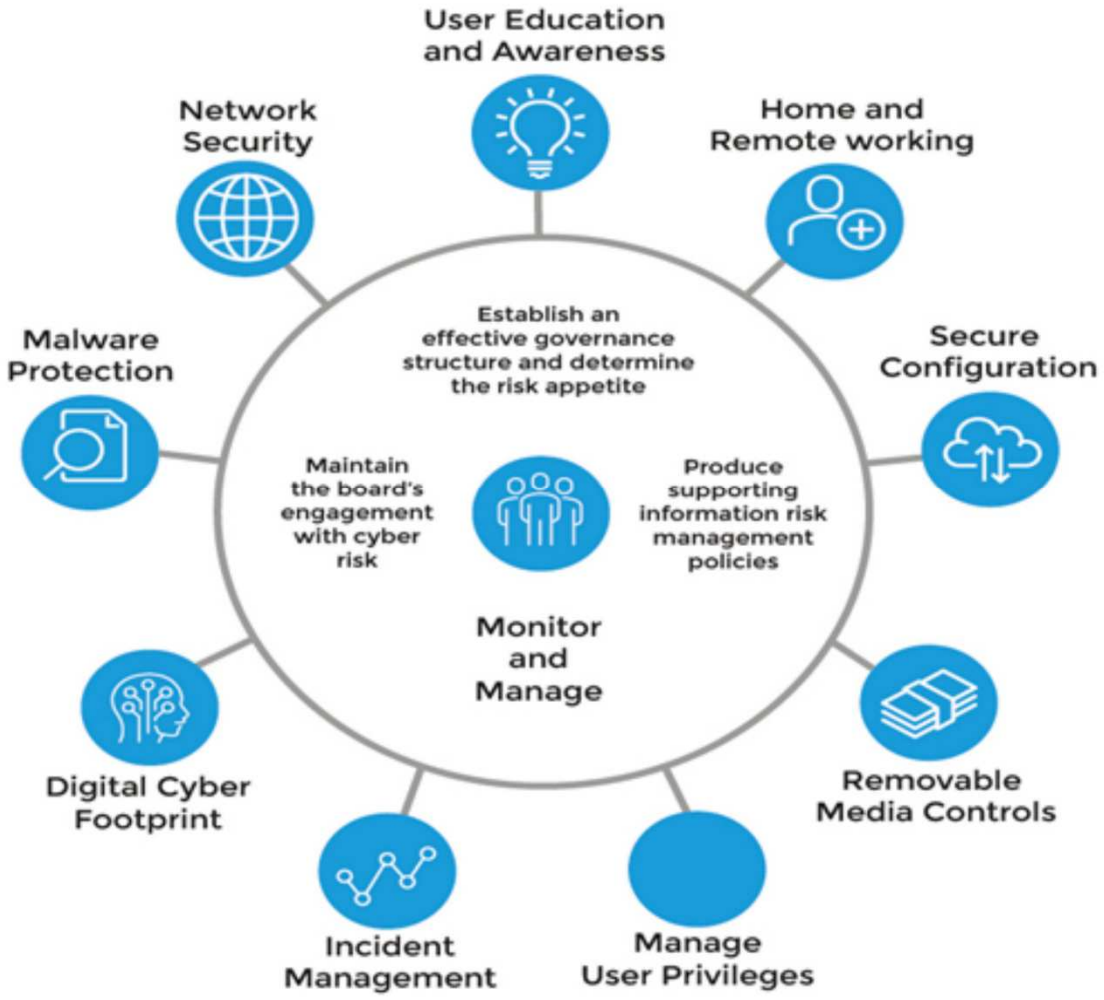
સંઘ પ્રદેશ દાદરા અને નગર હવેલી અને દમણ અને દીવ

UT OF DADRA AND NAGAR HAVELI AND DAMAN AND DIU

Cyber Security Management Plan V1.0



INDEX

Sl. No.	Contents	Page No.
	CYBER SECURITY POLICY	
1	Introduction	1
2	Purpose	1
3	Objective	2
4	Mandate	2
5	Scope	2
6	Definitions	2
7	Governance	4
7 a	Senior Management	4
7 b	Chief Information Security Officer (CISO)	5
8	Policy Development and Management	6
8.1	Cyber Policy Management	7
8.2	Security roles and responsibilities	7
8.3	Employee internet usage	7
8.4	Guidance on social media usage	8
8.5	Baseline cyber security/ resilience	8
8.6	Identification of potential reputation risk	10
9	Facility Security	10
9.1	Premises level security	10
9.2	Risk assessment of the premises	12
9.3	Ensuring Protection against environmental threats	13
9.4	Equipment protection	13
9.5	Cabling security	14
9.6	Equipment maintenance	15
9.7	Off-premises security of equipment's	15
9.8	Secure removal of equipment	15
9.9	Fire suppression and detecting systems	16
9.10	Training employees in facility security procedures	16
10	Employees Security	17
10.1	On-boarding of employees and third-party staff	17
10.2	Screening of employees and third-party staff	17
10.3	Information security awareness, education and training	18
10.4	Disciplinary process for information security breaches	18
10.5	Employee Transfer, Termination/superannuation	18
11	Application and hardware security	20
11.1	Device security	20
11.1.1	Asset identification and authentication	20
11.1.2	Asset security	21
11.1.3	Maintaining, monitoring and analyzing logs	21
11.2	Prevention of unauthorized software	22
11.3	Perimeter protection	22
11.4	Hardening of hardware and software	23
11.5	Network device protection	24
11.6	Application Security	24

11.7	Penetration testing	27
11.7.1	Development of Red Team	27
11.7.2	Penetration testing of infrastructure	28
11.7.3	Penetration testing of web application	29
11.7.4	Application Security testing of web application	29
12	Operational Security	30
12.1	Cyber Plan action items	31
12.1.1	Identity of critical information	31
12.1.2	Analysis of threats	31
12.1.3	Analysis of vulnerabilities	32
12.1.4	Assessment of risk	32
12.1.5	Application of appropriate OPSEC measures	33
13	Network Security	34
13.1	Internet access	34
13.2	Email access	34
13.3	Firewall security	35
13.4	Logging of network devices	37
13.5	Network monitoring	37
13.6	Dynamic host configuration protocol	38
13.7	Remote access-virtual private network	38
13.8	Wireless access	38
13.9	Patch management for network devices	39
13.10	Change management	39
13.11	Clock synchronization	40
13.12	Enforcement	40
13.13	Sustenance	40
14	Communication Management	41
14.1	Encryption	41
14.1.1	Use of encryption	41
14.1.2	Digital signatures	42
14.1.3	Key management	43
14.2	Information exchange agreements	43
14.3	Publicly available information	44
14.4	Email, internet and other electronic communication	44
14.4.1	Business use	44
14.4.2	Use of encryption	45
14.4.3	Acceptable use	45
14.4.4	Retention/ deletion of electronic mail	45
14.4.5	Personal websites	46
14.4.6	Social and professional networking media	46
14.5	Voice, FAX and video communications	46
14.5.1	Acceptable use	47
14.5.2	Phone calls	47
14.5.3	Voice mails	47
14.5.4	Facsimile	48
14.5.5	Conference calls/ video teleconferences	48
14.6	Meetings and conversations	48
14.6.1	Conference calls/ video teleconferences	48s

14.6.2	Public conversations	49
15	Incident Management	49
15.1	Reporting security weaknesses	50
15.2	Cyber Security Operation Centre (C-SOC)	50
15.3	Responding to information security incidents & weaknesses	52
15.4	Management of information security incidents & improvements	52
15.5	Remedies to information security incidents & weaknesses	53
15.6	Monitoring confidentialities for information security incidents	54
15.7	Collection of evidence of information security incidents	54
15.8	Ensuring Integrity of information security incident investigations	54
16	Problem Management	55
17	Capacity Management	55
18	Access Management	56
18.1	Business requirement of access control	56
18.2	User registration and deregistration	56
18.3	Privileged access management	57
18.4	Input control	57
18.5	User responsibilities	58
18.5.1	Password use or management	58
18.5.2	Unattended user equipment	59
18.5.3	Clear desk and clear use policy	60
18.6	Review of user access rights	60
18.7	Logging and monitoring activities	60
18.8	Administrator password management	61
18.9	Secure log-on procedures	61
18.10	Use of privileged utilities	61
18.11	Application and information access control	61
18.12	Session time out	62
18.13	Mobile computing	62
18.14	Citizen authentication	62
19	Antivirus Management	62
19.1	Antivirus updates	63
19.2	Scanning Government’s computing devices	63
19.3	Rules for virus prevention	63
20	Social Engineering- Protection against online fraud	64
20.1	Training employees to recognize social engineering	64
20.2	Protection against phishing	65
20.3	Avoid installation of fake antivirus	66
21	Protection against Malware	66
22	Systematic approach for protection against malicious software	66
23	Third Party security	67
24	Cloud Security	69
25	Disaster Recovery	71
25.1	Data backup and recovery plan	71
25.2	Disaster Recovery	72
25.3	Contingency Planning	73
26	Mobile Device security	74
26.1	Cyber Plan action items	74

27	Internet Banking and Other Transaction Security	75
28	Data Leakage Prevention	76
39	Removable Media Security and BYOD (Bring Your Own Device)	77
30	Cyber Audits	79
30.1	Cyber Security audit	79
30.1.1	Planning a cyber security audit	79
30.1.2	Execution of cyber security audit	79
30.1.3	Reporting and follow up	80
30.2	Compliance with security recommendations	80
30.3	Learning and evolving	80
31	Awareness	81
31.1	User/ employee awareness	81
31.2	Citizen awareness	82
32	Child Online Privacy Protection Act (COPPA).	83
33	Exceptions	86
34	Non-Compliance	86
35	Policy Review	86
	CYBER CRISIS MANAGEMENT PLAN	
1	Introduction	87
2	Authority	87
3	Purpose and scope	88
4	Audience	88
5	Cyber incident response capabilities	89
6	Cyber Incident Response Team (CIRT)	89
6.1	Mission of CIRT	90
6.2	Role and responsibilities of CIRT	90
7	Strategy and goals for cyber incident response	90
8	Protection and resilience of organization's infrastructure	91
9	Mock Drills to test preparedness to withstand cyber attacks	93
10	Reporting a cyber incident	93
11	Incident response processes	95
11.1	Preparation	95
11.2	Identification, detection and analysis	95
11.3	Forensic analysis	96
11.4	Common categories of cyber incidents	97
11.5	Containment, Eradication and Recovery	99
11.5.1	Containment	99
11.5.2	Eradication	100
11.5.3	Recovery	100
11.5.4	Incident Closure	101
	Annexure-1 : Guidance on Reporting a Cyber	102
	Annexure-2 : UT Helpdesk (DNH & DD) for reporting Cyber Incidents.	103
	Annexure-3 : Cert-In contacts details for reporting (Central Help Desk).	103
	Annexure-4 : Cert-In incident report form.	104
	Annexure-5 : Booklet Cyber Security Awareness for Citizens.	105

1. Cyber Security policy

1. Introduction

Use of Information Technology by Government and their constituents has grown rapidly and has now become an integral part of the operational strategies of Central/State/UTs Government. On the other hand, cyber security has become a major concern over the past few years as hackers have penetrated the IT infrastructure of the organization with increasing frequency and sophistication. Also, As AI/ML evolves, concerns about data privacy and risk management for both individuals and businesses continue to grow. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space. These developments have underlined the urgent need to put in place a robust cyber security/resilience framework at State Government and to ensure adequate cyber-security preparedness among Government entity on a continuous basis.

In view of the low barriers to entry, evolving nature, growing scale/velocity, motivation and resourcefulness of cyber-threats to the system, it is essential to enhance the resilience of the government system by improving the current defences in addressing cyber risks. These would include, but not limited to, putting in place an adaptive Incident Response, Management and Recovery framework to deal with adverse incidents/disruptions, if and when they occur.

2. Purpose

In order to address the need for the entire Government entity to contribute to a cyber-safe environment has guided that the Cyber Security Policy should be distinct and separate from the broader IT policy/Government Security policy so that it can highlight the risks from cyber threats and the measures to address/mitigate these risks.

The Cyber Security Policy put forth by the UT Administration of DNH and Daman & Diu, articulates management direction for addressing Cyber Security crisis management plan. The policy takes into consideration the guidelines from Government Authority {circular – F. No. 1(5)/ 2021)} dated 22/05/2024 and important security controls for effective cyber security as articulated by CERT-In (Computer Emergency Response Team-India, a Govt. entity).

This Cyber Security Policy is a formal set of rules by which those people who are given access to UT Administration of DNH and Daman & Diu organization technology and information assets must abide. The Cyber Security Policy serves several purposes. The main purpose is to inform government users i.e. employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the government.

3. Objective

The Cyber Security Policy describes the technology and information assets that must be protected and identifies the various threats to those assets. It also describes the user's responsibilities and privileges. The policy answers questions such as 'What is considered acceptable use?', 'what are the rules regarding Internet access?' etc., describes user limitations and informs users that there will be penalties for violation of the policy. The document also contains guidelines on responding to incidents that threaten the security of the government computer systems and network.

Main objective is to Protect society, the common good, necessary public trust and confidence, and the infrastructure.

4. Mandate

Ministries/Departments of Central Govt., State Government and Union Territories to draw-up their own sectoral Cyber Crisis Management Plans in line with the Cyber Crisis Management Plan for countering cyber-attacks and cyber terrorism.

Equip themselves suitable for implementation, supervise implementation and ensure compliance among all the organizational units (both public & private) within their domain.

CERT-in/MeitY to conduct mock drills with Ministries/organizations.

MeitY to seek necessary compliance information on implementation of the best IT security practices from all the organizational units of the Ministries/Departments of Central Government, State Government and Union Territories on a regular basis and apprise the NCMC of progress.

5. Scope

This policy applies to employees, contractors, consultants and other workers at the government and their associates, including all personnel affiliated with third parties. This policy also applies to all applications and equipment that is owned, leased or hired by the UT Administration of DNH and Daman & Diu.

6. Definitions: The acronyms and some of terms used in this policy are defined below:

a) Asset: Anything that has value to the organization.

b) Control: Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature.

c) Guideline: A description that clarifies what should be done and how, to achieve the objectives set out in policies.

d) Internet: Internet is the single, interconnected, worldwide system of commercial,

governmental, educational, and other computer networks.

e) Intranet: A private network that is employed within the confines of a given enterprise.

f) Information Processing Facilities: Any information processing system, service or infrastructure, or the physical locations housing them.

g) Information Security: Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non – repudiation, and reliability can also be involved.

h) Information Security Event: An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

i) Information Security Incident: An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

j) Business Continuity: is a state of continued and uninterrupted operation of business.

k) Business Continuity Management: is a holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely manner in the event of disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.

l) Business Continuity Plan: is a comprehensive, documented plan of action that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organization in the event of a disruption.

m) CISO: is an acronym referring to the Chief Information Security Officer. He/ She is the senior-level executive within an institution responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

n) Critical Information Infrastructure (CII): refers to interconnected information systems and networks, the disruption of which would have serious impact on the economic well-being of citizens, or on the effective functioning of payment service provider and the economy.

o) Cybersecurity incident: is any malicious act or suspicious event that: compromises, or attempts to compromise, the electronic security perimeter or physical security perimeter of a critical Cyber Asset or disrupts or attempts to disrupt, the operation of a critical Cyber Asset.

p) Cybercrime: according to the International Organization of Securities Commissions (IOSCO), ‘cyber-crime’ refers to a harmful activity executed by an

individual or a group, through computers, Information Technology (IT) systems and/or the internet and targeting the computers, IT infrastructure or internet presence of another entity.

q) Cybersecurity: is an activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized access or modification, or exploitation.

r) Cyber risk: is any risk arising from a failure of an institution's information technology systems resulting to financial loss, disruption of service, and/or interference with business as usual or damage to the reputation of an institution.

s) Cyberspace: is the virtual space created by interconnected computers and computer networks on the internet.

t) IT Infrastructure: refers to the hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and or citizens and is usually internal to an organization and deployed within owned facilities.

u) Red Team Exercise': refers to an all-out attempt to gain access to a system by any means necessary, and usually includes cyber penetration testing, physical breach, testing all phone lines for modem access, testing all wireless and systems present for potential wireless access and also testing employees through several scripted social engineering and phishing tests. These are real life exercises carried out by an elite small team of trained professionals that are hired to test the physical, cyber security, and social defenses of particular systems.

7. Governance

a) Senior Management

Senior Management of the UT Administration of DNH and Daman & Diu shall play its responsibility for implementing the government strategy in line with its risk appetite, while being cognizant of cyber threats. As such, the Senior Management will ensure to:

i) Implement the board approved cybersecurity strategy, policy and framework.

ii) Understand cyber organizational scope as well as identify cyber threats, critical business processes and assets.

iii) Ensure the creation of mitigation and recovery procedures to contain cyber risk incidents, reduce losses and return operations to normal.

iv) Continuously improve collection, analysis, and reporting of cybercrime information. This can be achieved through understanding the government working

environment, potential cyber risk points and referring to the guidelines of the regulator and adopting best practices tools available.

v) Oversee deployment of strong authentication measures to protect citizen data, transactions and systems.

vi) Ensure the provision of sufficient number of skilled staff for the management of cybersecurity, who should be subjected to enhanced background and competency checks.

vii) Ensure timely and regular reporting to the cyber security board on the cyber risk status of the institution.

viii) Incorporate cybersecurity as a standard agenda in Senior Management meetings and provide regular reports of the government cybersecurity posture to the board.

ix) Document cybersecurity incident response plan providing a roadmap for the actions the UT Administration of DNH and Daman & Diu will take during and after a security incident.

x) Create a post incident analysis framework to determine corrective actions to prevent recurrence of the incidents in the future.

xi) Oversee the evaluation and management of risks introduced by third party service providers; UT Administration of DNH and Daman & Diu may require attestation/assurance reports provided by reputable independent auditors for service providers.

b) Chief Information Security Officer (CISO)

As cyber-attacks evolve, one of the modern strategic measures globally accepted and acknowledged is the introduction of the role of the Chief Information Security Officer (CISO). This role is aimed at creating an organizational culture of shared cybersecurity ownership. Ultimate responsibility for implementing this policy shall rest with the CISO of the UT Administration of DNH and Daman & Diu. He/ She will be a senior level executive not below the rank of Assistant Director. CISO will report to the Director concerned or the Secretary of the UT Administration of DNH and Daman & Diu.

The CISO is responsible for:

i) Overseeing and implementing the UT Administration of DNH and Daman & Diu cybersecurity programme and enforcing the cybersecurity policy.

ii) Ensuring that the UT Administration of DNH and Daman & Diu maintains a current Government-wide knowledge base of its users, devices, applications and their relationships.

iii) Ensuring that information systems meet the needs of the UT Administration of DNH and Daman & Diu and the ICT (Information and Communication Technology)

strategy, in particular information system development strategies, comply with the overall business strategies, risk appetite and ICT risk management policies of the UT Administration of DNH and Daman & Diu.

iv) Design cybersecurity controls with the consideration of users at all levels of the organization, including internal (i.e. management and staff) and external users (i.e. contractors/consultants, business partners and service providers).

v) Organizing professional cyber related trainings to improve technical proficiency of staff.

vi) Ensure that adequate processes are in place for monitoring IT systems to detect cybersecurity events and incidents in a timely manner.

vii) Reporting to the competent authority on an agreed interval but not less than once per quarter on the following:

- Assessment of the confidentiality, integrity and availability of the information systems in the UT Administration of DNH and Daman & Diu.
- Detailed exceptions to the approved cybersecurity policies and procedures.
- Assessment of the effectiveness of the approved cybersecurity programme.
- All material cybersecurity events that affected the UT Administration of DNH and Daman & Diu during the period.

viii) Ensure timely update of the incident response mechanism and Business Continuity Plan (BCP) based on the latest cyber threat intelligence gathered.

ix) Incorporate the utilization of scenario analysis to consider a material cyber-attack, mitigating actions, and identify potential control gaps.

x) Ensure frequent data backups of critical IT systems (e.g. real time back up of changes made to critical data) are carried out to a separate storage location.

xi) Ensure the roles and responsibilities of managing cyber risks, including in emergency or crisis decision-making, are clearly defined, documented and communicated to relevant staff.

xii) Continuously test disaster recovery and BCP arrangements to ensure that the government can continue to function and meet its regulatory obligations in the event of an unforeseen attack through cyber-crime.

8. Policy Development & Management

The UT Administration of DNH and Daman & Diu is in the process of developing and maintaining clear and robust policies for safeguarding critical government data and sensitive information, protecting its reputation and discouraging inappropriate behavior by employees. Many of these types of policies already exist for “real world” situations, but shall be updated to reflect the increasing impact of cyberspace on everyday transactions, both professional and personal.

As with any other government document, cyber security policies shall follow good design and governance practices -- not so long that they become unusable, not so vague that they become meaningless and reviewed on a regular basis to ensure that they stay pertinent as the business needs change.

8.1 Cybersecurity Policy Management

To counter ever evolving cyber landscape and with adherence to Government of India Guidelines, the UT Administration of DNH and Daman & Diu has developed this robust cybersecurity policy document. The UT Administration of DNH and Daman & Diu has identified Chief Information Security Officer (CISO) as the custodian of Cybersecurity Policy. He will hold the primary responsibility to maintain the policy document in both electronic and paper format. He will also be responsible for the communication of the Policy in appropriate format like emails, intranet posting etc. to all employees and contractors of UT Administration of DNH and Daman & Diu. UT Administration of DNH and Daman & Diu IT Sub Committee of the Board shall review the Policy annually to assess its effectiveness and implementation. In annual meeting management shall analyze latest evolving threats in the cyber world and recommend necessary changes in the cybersecurity policy. Any change in cyber security procedure followed by UT Administration of DNH and Daman & Diu shall be updated in the Annual review process before rollout of the changes. The Government may conduct ad hoc policy review if deemed necessary due to any new guideline or high-profile evolving threat to organization whenever they occur.

8.2 Security roles and responsibilities

The Government shall establish procedures that clearly define the separation of roles and responsibilities with regard to systems and the information they contain. Such procedures need to clearly state, at a minimum:

Clearly identify UT Administration of DNH and Daman & Diu data ownership and employee roles for security oversight and their inherit privileges, including: Necessary roles, and the privileges and constraints accorded to those roles, the categories of employees who should be allowed to assume the various roles. How long an employee may hold a role before access rights must be reviewed. If employees may hold multiple roles, the circumstances defining when to adopt one role over another.

8.3 Employee Internet usage

The UT Administration of DNH and Daman & Diu shall define acceptable usage of internet for its employees. Following are the key policy statements for internet usage:

- Employees given internet access are expected to use the internet to enhance the performance of their job responsibilities. The data and information available on the Internet provides invaluable information, which can impact the necessary skill to enhance professional competence
- Employees given internet access are also responsible for assisting the UT Administration of DNH and Daman & Diu in identifying positive organizational

uses from the internet. Beneficial uses include availability of immense work-related information / updates of licensed products, facilities of special online services/ features, etc

- If a web filtering system is used by the UT Administration of DNH and Daman & Diu in the future, employees should have clear knowledge of how and why their web activities will be monitored, and what types of sites are deemed unacceptable by the UT Administration of DNH and Daman & Diu policy.

8.4 Guidance on social media usage

Social networking applications present a number of risks that are difficult to address using technical or procedural solutions. The UT Administration of DNH and Daman & Diu shall develop social media guidelines that will clearly include the following:

- Specific guidance on when to disclose UT Administration of DNH and Daman & Diu activities using social media, and what kinds of details can be discussed in a public forum.
- Additional rules of behaviour for employees using personal social networking accounts to make clear what kinds of discussion topics or posts could cause risk for the government.
- Guidance on the acceptability of using a government email address to register for, or get notices from, social media sites. Guidance on selecting long and strong passwords for social networking accounts, since very few social media sites enforce strong authentication policies for users. Lastly, all employees of the UT Administration of DNH and Daman & Diu shall be made aware of the risks associated with social networking tools and the types of data that can be automatically disclosed online when using social media. The UT Administration of DNH and Daman & Diu shall educate employees on the potential pitfalls of social media use, especially in tandem with geo-location services, may be the most beneficial social networking security practice of all.

8.5 Baseline Cyber Security/Resilience

UT Administration of DNH and Daman & Diu shall establish baseline cyber security requirements which shall be evaluated periodically to integrate risks that arise due to newer threats, products or processes.

8.5.1. Baseline Controls

- The government shall implement appropriate controls to protect Assets, including government data/information including citizen data/information, government applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc.
- The UT Administration of DNH and Daman & Diu shall take proper measures to Prevent execution of unauthorized software.
- The UT Administration of DNH and Daman & Diu shall put in place environmental controls for securing location of critical assets providing protection from natural and man-made threats

- The UT Administration of DNH and Daman & Diu shall ensure that all the network devices are configured appropriately and periodically assessed.
- The UT Administration of DNH and Daman & Diu shall document and apply baseline security requirements/configurations to all categories of devices throughout the lifecycle (from conception to deployment) and carry out reviews periodically
- The UT Administration of DNH and Daman & Diu shall ensure information security across all stages of application life cycle.
- The UT Administration of DNH and Daman & Diu shall follow a risk based strategy for Patch/Vulnerability & Change Management
- The UT Administration of DNH and Daman & Diu shall ensure secure User Access Control / Management
- The UT Administration of DNH and Daman & Diu shall implement secure mail and messaging systems
- The UT Administration of DNH and Daman & Diu shall ensure appropriate management and assurance on security risks in outsourced and partner arrangements
- The UT Administration of DNH and Daman & Diu shall implement policy for restriction and secure use of removable media
- The UT Administration of DNH and Daman & Diu shall build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise
- The UT Administration of DNH and Daman & Diu shall develop and implement a comprehensive data loss/leakage prevention strategy
- The UT Administration of DNH and Daman & Diu shall implement and periodically validate settings for capturing of appropriate logs/audit trails
- The UT Administration of DNH and Daman & Diu shall periodically conduct vulnerability assessment and penetration testing exercises
- The UT Administration of DNH and Daman & Diu shall put in place a fully effective Incident Response programme to respond to cyber incidents
- The UT Administration of DNH and Daman & Diu shall implement risk based transaction monitoring or surveillance process
- The UT Administration of DNH and Daman & Diu shall develop a comprehensive set of metrics that provide for prospective and retrospective measures
- The UT Administration of DNH and Daman & Diu shall have proper arrangements for network forensics/forensic investigation
- The UT Administration of DNH and Daman & Diu shall ensure employee/user/citizen awareness on baseline cyber security measures.

8.6 Identification of potential reputation risks

The UT Administration of DNH and Daman & Diu shall identify potential risks to their reputation and develop a strategy to mitigate those risks via policies or other measures as available. Specific types of reputation risks include:

- Being impersonated online by a criminal organization (e.g., an illegitimate website spoofing government name and copying government site design, then attempting to defraud citizens via phishing scams or other method).
- Having sensitive government or citizens information leaked to the public via the web.
- Having sensitive or inappropriate employee actions made public via the web or social media sites.

UT Administration of DNH and Daman & Diu shall take appropriate measures for identifying potential risks to the organization's reputation in cyberspace, practical measures to prevent those risks from materializing and reference plans to respond and recover from potential incidents as soon as they occur.

9. Facility Security

Protecting employees and members of the public who visit the government facility is a complex and challenging responsibility. It's also one of the UT Administration of DNH and Daman & Diu top priorities. The Facility Security Policy provides direction for the development and implementation of appropriate security controls that are required for protection of all information assets and processing facilities of the UT Administration of DNH and Daman & Diu from physical and environmental threats.

Following are the key Cyber Plan Action Items:

9.1 Premises Level Security

The purpose of Premises Level Security is to ensure the physical security of premises and assets of the UT Administration of DNH and Daman & Diu and create a secure climate that deters criminal activity.

Policy Statement

The walls and doors to the government are the first layer of defence against individuals gaining unauthorized entry. Consequently, it is important that walls and doors are of robust construction and do not allow a potential intruder easy access. The security perimeters for Organization buildings must be well defined and physically sound. External doors of Organization areas must be suitably protected against unauthorized access. Access to sites and building to be restricted to authorized users and appropriate control mechanism should be in place.

Security controls relating to any employee or non-government employees visiting an organization premises should include but not be limited to, the following:

- Critical areas like Data Centre, Disaster Recovery Centre etc. shall be manned by security guard(s) on 24*7 basis.

- Data Centre and Disaster Recovery Centre visitors shall be appropriately logged when entering the building.
- With the exception of publicly accessible / open areas (e.g. branches), all visitors must be escorted by an employee, not including those third-party contractors who have been screened and granted an access pass to government premises.
- Security guard deployed at the government premises should keep an eye on all personnel entering and leaving the premises. Any suspicious activity should be immediately reported to the respected authority.
- Access rights to secure areas should be regularly monitored, reviewed, updated and revoked when necessary.
- Need of access to Secured area to employees as well as third party employees from enabling functions shall be assessed & approved by the concerned premises in charge. The list of such accesses shall be sent to CISO for review on quarterly basis.
- All employees must be issued an employee identification card, with photograph, that must be worn visibly at all times and checked when entering government premises. This is applicable at the secretariat, collectorate offices, and other government offices which are required to be secured.
- Access to areas hosting information classified as SECRET or data Centre, server rooms and hub rooms must be restricted only to employees who are authorized to have access to those areas. Such areas must be situated away from public areas. Access must be controlled through appropriate access control and authentication mechanisms e.g. proximity-based access control system, electronic keypad or biometric.
- In addition, audit control logs, detailing access, must be periodically reviewed and stored for a minimum period of 90 days.
- Vendors or visitors requiring access to secure areas, such as data centre, server rooms and hub rooms, who have not been vetted using the standard government employees vetting procedures, must be escorted at all times by an authorized member of employees.
- In addition, their access must be recorded in a visitor/vendor tracking book and be pre-authorized by relevant employees. All external access doors, including fire doors, must be fitted with alarms and close and open effectively. They must never be propped open unless continuously monitored by employee or authorized security personnel.
- Specific areas such as server rooms, information processing facilities, and certain offices depending on their criticality and risk exposure, should be categorized as ‘secure areas’ and appropriate controls should be implemented. Such secure areas should have additional controls implemented including, but not limited to:
    - Vacant secure areas should be locked and periodically checked.
    - Unsupervised working in the secure areas should be avoided both for health and safety reasons, and to prevent any potential malicious activities.
    - Premises & common passage area shall be monitored & recorded 24x7 using CCTV surveillance cameras may be by security guards.

Recording shall be preserved for 90 days.

- The CCTV cameras must be positioned in such a way that they record the face of individuals entering the area concerned (i.e. looking in to out) and must be capable of producing images of sufficient quality to allow facial recognition. The cameras are to be connected to a reliable recording device set to record continuously. Sufficient lighting must be considered in order to allow cameras to clearly record activities in the hours of darkness or in inclement weather conditions.
- Review of all left/absconded employees shall be done at least once a quarter.
- Removal of Access Levels
    - Access shall be removed for relieved employee on the last working day.
    - Access shall be removed for the absconded employee immediately on HR notification.
    - Removal of access at the time of change in location immediately before providing access to new premise.

9.2 Risk Assessment of the Premises.

Risk assessment of the premises of the government should be carried out in order to identify, analyze evaluate and treat the risk of disruptive incidents to the organization.

Policy Statement

- UT Administration of DNH and Daman & Diu shall maintain a list of identified risk for premise level security. This list shall be updated as and when a new risk is identified. The new risk shall be identified during risk assessment or as and when a new security incident has occurred in government.
- UT Administration of DNH and Daman & Diu shall proactively participate on CISO forums, register to risk advisory from various organizations like CERT-In, NCR&IC (National Cybercrime Research & Innovation Center), I4C (Indian Cybercrime Coordination Centre) etc. to keep apprised itself about new emerging cyber security risks, and shall take appropriate measures to mitigate such risks.
- UT Administration of DNH and Daman & Diu shall conduct risk assessment of the sites selected for information storage, processing and boarding the government employees shall be performed periodically to ensure effectiveness of controls which are in place to mitigate, avoid or transfer any impact of risks arising from threats exploiting any and all known vulnerabilities.
- Periodic risk assessment report shall be developed which highlight risk and control effectiveness. This will in turn enhance the confidentiality, integrity, and resilience level of organization by treating the identified risks appropriately. It shall also highlight effectiveness of controls in arresting a threat from exploiting vulnerability, probability of occurrence of a potential threat.

- UT Administration of DNH and Daman & Diu shall take appropriate remediation measures to improve control deficiencies identified during risk assessment phase. Remediation measure may involve improve existing control or developing new controls based on details of control deficiencies and its implication to security measure.

9.3 Ensuring Protection against Environmental Threats

Physical protection against damage from natural or man-made disasters such as fire, flood, earthquake, explosion and civil unrest that are appropriate to the location shall be developed and implemented appropriately.

Policy Statement

- When locating equipment, computers and other hardware, suitable precaution shall be taken to guard against the environmental threats of fire, flood and excessive ambient temperature / humidity.
- All installations must be provided with appropriate heat, humidity, fire and smoke detection equipment as also fire extinguishers, dehumidifiers and air conditioners. Air conditioning and humidity controls must be installed in the computer room, and these controls must operate continuously and be available 24 hours per day. The air conditioning equipment shall incorporate machine redundancy such that the failure of any one component shall not interrupt the air conditioning.
- The effectiveness for such installations shall be reviewed at least on monthly basis through sample testing, as applicable. Hazardous or combustible material shall be stored at an adequate distance away from critical assets to avoid damage.

9.4 Equipment Protection

Suitable precaution shall be taken to protect the government equipment, such as, but not limited to, computers, laptops and supporting utilities and from environmental threats and hazards like flood, fire, power failures, excessive temperature / humidity and unauthorized access. All necessary steps for ensuring environmental safety such as regular cleaning, dusting (with due care for equipment safety), or prohibition of drinking & eating near the electronic equipment – must be taken.

- Server and Networking Equipment
    - The Production servers and the other network devices shall be kept in data Centre/communication rooms/hub rooms preferably at the central place.
    - These rooms shall be protected with an access control mechanism and shall be accessible to authorized personnel only.
- Laptops and Desktops
    - All desktops of the company shall be located within company-defined locations to protect from physical damage, theft and unauthorized access.

- All government provided laptops must be used for official purpose only.
- Laptop owners shall ensure the physical safety of device in public places.

- Power Supply
  - A backup UPS system/s and/or Generator/s will be installed. Desktop PCs and other equipment shall be connected to UPS depending on need. The specifications of the UPS shall be reviewed at least once a year for adequacy of capacity and to check for any gross over specification. An annual maintenance contract with SLAs defined shall be entered into with an agency for the UPS and the Generator

9.5 Cabling Security

The security of cabling should be considered for the existing setup and subsequently, when hardware enhancements are carried out. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

Policy Statement

- Cables are to be physically concealed (within wall, floor or ceiling cavities) wherever possible. Mission critical cables and those for security systems must be adequately protected to ensure that they are not subject to accidental or deliberate damage or interference. Examples of cables potentially requiring protection include:
  - Critical data cables in between buildings.
  - Cables for CCTV, Automatic Access Control Systems and alarm systems.
  - Power Cables from Standby generators/air conditioners.

Wherever possible, such cables are to be physically concealed (buried underground to a depth of at least 1 meter if outside or concealed within wall, floor or ceiling cavities within the premises).

- Critical data and system cables that are exposed and accessible to non-government personnel must be concealed in steel conduits. The steel conduits must be tamper proof and should not be marked to identify the conduit as containing government cables or the function of the cables (e.g. CCTV etc.).
- Exposed critical cables within government premises are to be placed in conduit or ducting to ensure that they are protected from accidental damage.
- Service/maintenance ducts giving access to critical system cabling should be secured using high quality security padlocks or other appropriate means.
- Wherever possible, consideration should be given to having mission critical data cables accessible to non-government staff (i.e. in shared building or where there is a physical connection between buildings) monitored by an alarm system capable of detecting various forms of physical attacks (such as cutting, drilling, hammering, etc.). The alarm monitoring should begin at the conduits rather than at the data cable. The alarm system must alert on a

change in condition of the conduit, so the alarm can be investigated immediately, on a 24/7 basis.

9.6 Equipment Maintenance

Suitable measures shall be taken to maintain the government equipments, such as, but not limited to, computers, laptops and supporting utilities to ensure continued usage and reliability.

Policy Statement

- All equipment should be serviced at regular intervals and as stipulated by any SLA and insurance contracts.
- Only authorized maintenance personnel should carryout repairs and service equipment.
- Adequate records of failures, faults, corrections or testing must be maintained.
- Failures and faults must be analyzed periodically and corrective action taken as appropriate.

9.7 Off-Premises Security of Equipment

Appropriate authorization, access control and protection shall be taken to reduce the risk of loss or destruction to an acceptable level, for equipment's that are stored or taken outside the organization's premises.

Policy Statement

- All equipment, including media containing CONFIDENTIAL or SECRET information, shipped out of their primary location should be protected both whilst in transit and when housed at any external location.
- Insurance arrangements should provide cover for equipment stored and used at offsite locations.
- Equipment should not be moved offsite without proper authorization.
- Security risks such as damage, theft or eaves dropping may vary considerably between locations and should be taken into account in determining most appropriate controls.

9.8 Secure Removal of Equipment

Computing systems generally store data on a wide variety of storage media. It is imperative that the data is securely removed from the media once the data or device is no longer needed to prevent unauthorized disclosure of the data.

Policy Statement

- The disposal or abandoning of major hardware must be authorized and approved first by the departmental head and finally by other competent authority depending upon the value involved and the decision must be based upon study of the reasons for disposing of the hardware.
- While disposing of hardware it must be ensured that all hard discs or other

media / memory attached to the hardware are fully formatted or cleared using

degauss machines, so that there is no compromise of confidential or private information and data/software on the same becomes irrecoverable.

- It must also be ensured that while formatting the discs / media, the important data / information is backed up or saved appropriately.
- Only authorized persons (vendor representatives / Government staff) – authorized by the departmental head – must be allowed to take the equipment belonging to government off the premises. They are responsible for its security at all times.
- All requirements imposed by insurance policies shall be complied with.
- Disposed Assets must be recorded as per the procedures followed by government for its Information inventory.
- Any critical document/media, while disposing must be shredded/physically destroyed with a view to make the same totally unrecoverable.

9.9 Fire Suppression and Detection Systems

Appropriate measures must be taken to install and maintain fire suppressors and detectors to ensure availability of adequate resources to guard information assets in the event of a fire.

Policy Statement

- All detection systems and related alarms – smoke detection, fire detection etc. shall be tested at least half yearly for their functionality.

9.10 Training employees in facility security procedures

A security breach of citizen information or a breach of internal departmental information can result in a public loss of confidence in the government and can be as devastating for government as a natural disaster. Hence, training employees in facility security procedures is very important to ensure that they are aware of the risks and precautionary measures to be taken.

Policy Statement

- In order to address such risks, government shall train the employees on the potential vulnerabilities and the procedures and practices that must be a standard part of each employee's workday.
- Security training should be stressed as critical and reinforced via daily procedures and leadership modelling.

10. Employee Security.

10.1 On-boarding of Employees and Third Party Staff

The UT Administration of DNH and Daman & Diu shall ensure that all employees and third party staff shall agree to and sign the terms and conditions of their employment contract which shall include the organization's responsibilities for information security.

Policy Statement

- The terms and conditions of employment shall include the employee's responsibilities for information security as laid down by the Information Security Policy.
- Employees of the UT Administration of DNH and Daman & Diu shall grant the government exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop.
- The confidentiality agreement shall be reviewed when there are changes to terms of employment or contract.
- All third party individuals / contractors shall be required to sign a confidentiality and nondisclosure agreement prior to any access to government Information & assets.

10.2 Screening of Employees and Third Party Staff.

Ineffective background check process could result in hiring of personnel with criminal/ dubious background. Hence, screening of employees and third party staff is essential before assigning them a position of responsibility.

Policy Statement

- Background screening on permanent staff, shall be carried out at the time of job applications as suitably carried out under HR Process.
- Information systems technical details, such as network addresses, network diagrams, and security software employed, shall not be revealed to job applicants (permanent employees & contractors) until they have been hired and have signed a confidentiality agreement.
- Persons who have a criminal conviction shall not be hired into, retained for, promoted into, or maintained in computer-related positions of trust.
- UT Administration of DNH and Daman & Diu shall obtain background verification reports from all third party personnel having access to government information assets and information processing facilities. In case of an exception, the employee shall be on-boarded only after obtaining an approval from head office HR department.

10.3 Information Security Awareness, Education and Training

Lack of awareness around information security requirements may lead to employees working on engagements not adhering to the same. The UT Administration of DNH and Daman & Diu Management shall ensure that all employees and third-party staff shall receive regular information security related trainings covering the policies, procedures, guidelines and any changes made thereof.

Policy Statement

- All employees of the organization and, where relevant, third-party users will receive appropriate training and regular updates in cyber security policies.
- All employees and contractors shall get information security training prior to being given access to information systems. The training program includes the relevant sections with appropriate Do's and Don'ts that the employees need to practice in their day-to-day work.
- In the event of changes to the security policies and procedures, same shall be communicated to all concerned employees and temporary workers / contractors. Security awareness programs shall be conducted on annual basis.

10.4 Disciplinary Process for Information Security Breaches

Information security breaches represent a persistent government risk and a disciplinary process must be followed for all such breaches.

Policy Statement

- Any non – compliance with or violation of the policy requirements shall result in disciplinary actions as per the government policy.
- The disciplinary actions shall depend on the context and gravity of the breach.

10.5 Employee Transfer, Termination/Superannuation

The employee transfer and termination responsibilities shall be in compliance with the defined procedures. Not following a mandated termination process could lead to unauthorized access by the terminated employee, modification/ deletion of critical data by the terminated employee, disclosing of critical information to rival companies or physical damage/ misplacement of hardware asset.

Policy Statement

- Human Resources or Administration shall notify departmental incharge about the transfer or termination of any employee of the organization without delay.
- In case of Transfer or cessation of third-party personnel or contractors, concerned department shall notify the other related departments. Unless the concerned department has received instructions to the contrary, two weeks

after an employee has permanently left the Company, all files held in that user's directories shall be purged.

- Email access of personal capacity, limited to Read access only, shall be provided to employees for a maximum of 30 days period from his/her last working date in superannuation cases. Otherwise, the access shall be revoked immediately after termination. In case any access is required to be maintained, appropriate approval shall be taken and maintained.
- Any email access of Organizational capacity shall be revoked immediately after termination/superannuation of employees.
- The password of generic user IDs shall be changed immediately after the termination of the owner of the ID.
- Government property including, but not limited to, portable computers, SIM cards, books, documentation, building keys, I-Card and magnetic access cards etc. will be returned at the time when an employee, contractor or third-party personnel leaves or when change in responsibilities occurs.
- System privileges and access to information and information assets to employee, contractor and third-party personnel shall be removed immediately (within 24 working hours) when user leaves the organization or in case of change in responsibility Information Security Policy which requires change in access. (In case any access is required to be maintained, appropriate approval shall be taken and maintained).

11. Application & Hardware Security

Appropriate consideration of Security at every stage of a system's development and installation of hardware and infrastructure can result in a resilient Cyber Infrastructure. Government must understand the importance to consider the security implications in software development from the inception stage as it's much easier to build security into a system than it is to add security onto an existing system.

Policy Statement

- Government shall consider physical and logical security of its hardware and IT Infrastructure with paramount importance as they house the government critical and sensitive information and processes. The security if compromised can result in high profile breaches which may impact reputation and day to day operation of Government.
- As the frequency and malignancy of cyber-attacks are increasing, it is imperative that UT Administration of DNH & Daman and Diu implements security solutions at the data, application, database, operating systems and networks to adequately address related threats.
- Appropriate measures shall be implemented to protect sensitive or confidential information such as citizen personal information, account and transaction data which are stored and processed in systems.
- Citizens shall be properly authenticated before access to online transactions, sensitive personal or account information.

11.1 Device Security

11.1.1 Asset Identification and Authentication

Identification of the asset, facilitates an organization to correlate different set of information about assets. Implementation of identification and authentication control of critical infrastructure can check and trace the misuse of the any asset. Absence of this control may lead to threats which may hamper the CIA (confidentiality, Integrity and availability) model.

Policy Statement

- The UT Administration of DNH and Daman & Diu shall review all the access controls for identification and disabling all users who are not associated with the organization.
- The UT Administration of DNH and Daman & Diu shall classify data/information based on information classification/sensitivity criteria of the government.
- Maintain an up-to-date inventory of Assets, including government data/information including citizens data/information, government applications, supporting IT infrastructure and facilities – hardware/software/network devices, key personnel, services, etc. indicating their government criticality.

11.1.2 Asset Security

Asset security focuses on collecting, handling, and protecting information throughout its life cycle. This includes sensitive information stored, processed, or transmitted on computing systems. Sensitive information is any information that an organization keeps private and can include multiple levels of classifications.

Policy Statement

- The UT Administration of DNH and Daman & Diu shall take specific steps to mark, handle, store, and destroy sensitive information, and these steps help prevent the loss of confidentiality due to unauthorized disclosure.
- The UT Administration of DNH and Daman & Diu shall commonly define specific rules for record retention to ensure that data is available when it is needed. Data retention policies also reduce liabilities resulting from keeping data for too long.
- The UT Administration of DNH and Daman & Diu shall protect the confidentiality of data using encryption to protect data both at rest and at transit
- UT Administration of DNH and Daman & Diu shall have appropriate controls in place to manage and provide protection of the IT assets within and outside its network. It shall take into consideration how the data/information is stored, transmitted, processed, accessed and put to use both within/outside the government network and the level of risk they are exposed to depending on the sensitivity of the data/information.
- UT Administration of DNH and Daman & Diu shall ensure changes to government applications, supporting technology, service components and facilities are managed using robust configuration. management processes and baseline that ensures integrity of any changes thereto. UT Administration of DNH and Daman & Diu shall develop detailed procedures about the change management to all types of assets.

11.1.3 Maintaining, Monitoring and Analyzing logs.

The control of log maintenance, monitoring and analysis is important for cyber-attack root cause analysis. The source for logs could be CCTV recordings, access systems, server logs, system logs, network protection devices logs, activity logs. Also, these logs may be useful to analyze the health of the complete organizational infrastructure.

Policy Statement

- The UT Administration of DNH and Daman & Diu shall monitor and configure security devices as per government policy for monitoring system access and use.
- The UT Administration of DNH and Daman & Diu shall retain user access logs as per regulatory requirements and periodic backup shall be conducted.

Backup logs to be stored in an encrypted format as per regulatory requirements.

11.2 Prevention of Unauthorized Software

UT Administration of DNH and Daman & Diu understand risk involved in installation of unauthorized software in any of government IT asset including desktop, laptop and all other handheld devices. To prevent unauthorized access government shall enforce below measures:

Policy Statement

- UT Administration of DNH and Daman & Diu shall maintain an up-to-date inventory of authorized software(s). • Government shall develop detailed procedure to restrict installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices and shall also implement mechanism to prevent installation and running of unauthorized software/applications on such devices/systems.
- UT Administration of DNH and Daman & Diu shall continuously monitor the release of patches by third parties i.e. vendors / OEMs, advisories issued by CERT-in and other similar agencies. Further the patches shall be applied as per the existing patch management practice of the government. UT Administration of DNH and Daman & Diu will also develop methodology to expeditiously apply an emergency patch, if patches are released by such third parties for protection against well-known attacks exploiting the vulnerability
- UT Administration of DNH and Daman & Diu shall have clearly defined framework to manage exceptions granted on a periodic basis by the senior management. Framework shall involve areas such as duration of exceptions, process of granting exceptions and authority for approving & review of exceptions

11.3 Perimeter Protection

Perimeter zone of an organization comprises of DMZ, NIPS, external routers, firewall, and proxy. This perimeter zone is mostly prone to external threats and attacks originating from outside the organizational network. Protection of perimeter zone includes routing security with well-designed hardening of the firewalls, proxies, network, etc.

Policy Statement

- The UT Administration of DNH and Daman & Diu shall implement system, application and database security to all internal infrastructure components.
- The UT Administration of DNH and Daman & Diu shall limit incoming access

to government data and systems from the Internet. This limit shall be implemented via use of a Demilitarized Zone (DMZ), which is a part of the firewall architecture. In no case shall access be granted to the public to access data directly on servers on the government's trusted network, which are inside of the firewall system.

- UT Administration of DNH and Daman & Diu shall centralize modem and Internet access to provide a consistent authentication process, and to subject the inbound and outbound network traffic.

11.4 Hardening of Hardware and Software.

The purpose of hardening is to reduce security risk arising due to surface vulnerabilities. This is typically done by disabling unnecessary services and removing all non-essential software programs and utilities. The government shall harden all the devices in production setup.

Policy Statement

- UT Administration of DNH and Daman & Diu shall develop and document security baselines for all types of information systems including all hardware and software on Laptops, Workstations, and Servers and Network Devices such as Firewalls, Routers and Switches
- UT Administration of DNH and Daman & Diu shall secure console port, auxiliary port, and connectivity management processor. In addition, all unused ports shall be closed.
- UT Administration of DNH and Daman & Diu shall disable IP source routing to avoid spoofing and attacks like Man-in- Middle (MIM).
- UT Administration of DNH and Daman & Diu shall develop privileged partition operating system hardening to secure the virtualization platform. This will be performed by 1) limiting VM resource use: set limits on the use of resources (e.g., processors, memory, disk space, virtual network interfaces) by each VM so that no one VM can monopolize resources on a system. 2) Ensure time synchronization: ensure that host and guests use synchronized time for investigative and forensic purposes.
- UT Administration of DNH and Daman & Diu shall implement various measures for host level hardening (including patch application and proper security configurations of the operating system (OS), browsers, and other network-aware software), considering implementing host-based firewalls on each internal computer and especially laptops assigned to mobile users. Many host-based firewalls also have application hashing capabilities, which are helpful in identifying applications that may have been affected after initial installation, considering host IPS and integrity checking software combined with strict change controls and configuration management.
- UT Administration of DNH and Daman & Diu shall ensure hardening of the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit.

11.5 Network Device Protection

The UT Administration of DNH and Daman & Diu IT network comprises of devices like routers, switches, IPS, firewalls, etc., these devices are exposed to internal and external vulnerabilities. Measures shall be taken for network monitoring, network performance management, and traffic measurement.

Policy Statement

- The UT Administration of DNH and Daman & Diu shall ensure that its network topology and architecture is aligned with the criticality of organization.
- The UT Administration of DNH and Daman & Diu shall conduct network configuration review once a year and shall confirm closure for the gaps identified during network review.
- All type of cables including UTP, fiber, power shall have proper labeling for further corrective or preventive maintenance works.
- The UT Administration of DNH and Daman & Diu shall ensure physical security of all network equipment's.
- Groups of information services, users and information systems shall be segregated in networks, e.g. VLAN.
- Unauthorized access and electronic tampering shall be controlled strictly. Mechanism shall be in place to encrypt and decrypt sensitive data travelling through WAN or public network.
- UT Administration of DNH and Daman & Diu shall implement network surveillance and security monitoring procedures (using SOC capabilities) with the use of network security devices, such as intrusion detection and prevention systems, to protect the Government against network intrusion attacks as well as provide alerts when an intrusion occurs.

11.6 Application Security

Secure systems are not just assembled; they are designed to support security. Security aspect should be embedded to system right from the design to rollout. Building security to a system is costly and inappropriate mechanism which can open new vulnerabilities. Also Security guidelines must be applied at each layer of web applications, servers, clients and communication channels. Web application security testing shall be conducted followed by closure of gap identified before go live.

Policy Statement

- UT Administration of DNH and Daman & Diu shall incorporate/ensure information security across all stages of application life cycle.
- In respect of critical government applications, UT Administration of DNH and Daman & Diu may consider conducting source code audits by professionally competent personnel/service providers or have assurance from application providers/OEMs that the application is free from embedded malicious / fraudulent code.
- Program/ Application development teams shall follow secure web application

design, coding practices.

- UT Administration of DNH and Daman & Diu shall clearly specify government functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling at the initial and ongoing stages of system development/acquisition/implementation.
- UT Administration of DNH and Daman & Diu shall segregate the development, test and production environments properly.
- UT Administration of DNH and Daman & Diu shall ensure that Software/Application development approach is based on threat modelling, incorporate secure coding principles and security testing based on global standards and secure rollout.
- UT Administration of DNH and Daman & Diu shall ensure that software/application development practices addresses the vulnerabilities based on best practices baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism. OWASP Top 10 Web Application Security mention below.
- UT Administration of DNH and Daman & Diu shall consider implementing measures such as installing a "containerized" app on mobile/smart phones for exclusive government use that is encrypted and separated from other smartphone data/applications; measures to initiate a remote wipe on the containerized app, rendering the data unreadable, in case of requirement may also be considered.
- UT Administration of DNH and Daman & Diu shall ensure that adoption of new technologies shall be adequately evaluated for existing/evolving security threats and IT/security team of the government reach reasonable level of comfort and maturity with such technologies before introducing for critical systems of the government.
- The UT Administration of DNH and Daman & Diu shall use appropriate cryptographic techniques to secure critical information code, database or logs.
- The UT Administration of DNH and Daman & Diu shall consider deploying web application firewall to filter and monitor inbound and out-bound traffic.
- The UT Administration of DNH and Daman & Diu shall conduct vulnerability assessment and penetration testing quarterly for all web facing applications and before Go-live of new web application.
- The UT Administration of DNH and Daman & Diu shall confirm closure for the gaps identified during vulnerability assessment.
- The UT Administration of DNH and Daman & Diu shall establish appropriate security monitoring systems and processes, to facilitate prompt detection of unauthorized or malicious activities by internal and external parties.
- The UT Administration of DNH and Daman & Diu shall implement security monitoring tools which enable the detection of changes to critical ICT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes.

- The UT Administration of DNH and Daman & Diu shall regularly review security logs of systems, applications and network devices for anomalies. Logs shall be protected and retained for defined period to facilitate future investigations.

Top 10 Web Application Security Risks.

- **A01:2021-Broken Access Control** moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021-Cryptographic Failures** shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.
- **A03:2021-Injection** slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021-Insecure Design** is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to "move left" as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.
- **A05:2021-Security Misconfiguration** moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021-Vulnerable and Outdated Components** was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis. This category moves up from #9 in 2017 and is a known issue that we struggle to test and assess risk. It is the only category not to have any Common Vulnerability and Exposures (CVEs) mapped to the included CWEs, so a default exploit and impact weights of 5.0 are factored into their scores.
- **A07:2021-Identification and Authentication Failures** was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks seems to be helping.
- **A08:2021-Software and Data Integrity Failures** is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts from Common Vulnerability and Exposures/Common Vulnerability Scoring System (CVE/CVSS) data mapped to the 10 CWEs in this category. Insecure Deserialization from 2017 is now a part of this larger category.
- **A09:2021-Security Logging and Monitoring Failures** was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This category is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.

- **A10:2021-Server-Side Request Forgery** is added from the Top 10 community survey (#1). The data shows a relatively low incidence rate with above average testing coverage, along with above-average ratings for Exploit and Impact potential. This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

11.7 Penetration Testing

With cyber-attacks becoming common, it is essential for organizations to undertake regular vulnerability scans and penetration testing to identify vulnerabilities and ensure on a regular basis that the cyber controls are working.

Policy Statement

- UT Administration of DNH and Daman & Diu shall periodically conduct vulnerability assessment and penetration testing exercises for all the critical systems, particularly those facing the internet. This section cover the details of Penetration testing. The vulnerabilities detected are to be remedied promptly in terms of the government cyber risk management/treatment framework so as to avoid exploitation of such vulnerabilities
- Penetration test is an attempt to exploit system vulnerabilities (including OS, service and application flaws, improper configurations etc.). It is also useful in validating the efficacy of defensive mechanisms, as well as end-users' adherence to security policies. These vulnerabilities can be discovered by penetration testing methodologies involving the usage of different sophisticated tools and processes.
- UT Administration of DNH and Daman & Diu shall ensure findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security team as well as Senior Management.
- UT Administration of DNH and Daman & Diu shall promptly remediate all vulnerabilities detected in terms of the government cyber risk management/treatment framework so as to avoid exploitation of such vulnerabilities.

11.7.1 Development of Red Team

A red team is an independent group that challenges an organization to improve its effectiveness and is essential in identifying potential risks.

Policy Statement

- UT Administration of DNH and Daman & Diu shall develop Red Team whose

members will be identified from Information Security Cell. The primary responsibility of this team will be to simulate acts of hacker. Red team members will perform penetration testing at infrastructure and at web application level.

- The objective of red team exercise is to identify the existing vulnerabilities in UT Administration of DNH and Daman & Diu network and application and its effectiveness of security measure. Team also have the responsibility to identify latest cyber hacking techniques proactively based on occurrence of same anywhere in world.
- Red Team may simulate the new techniques as and when deemed necessary to identify new vulnerabilities.

11.7.2 Penetration testing of Infrastructure.

An infrastructure penetration test is an important method of evaluating the security of the Government computing networks, infrastructure and application weaknesses by simulating a malicious attack

Policy Statement
UT Administration of DNH and Daman & Diu shall perform Penetration Testing at all four-level listed below for Infrastructure and Configuration Review

• **Level 1:** External Penetration Testing (Non-Intrusive) on External Devices / Servers

In this level, external non-intrusive penetration testing will be carried out to gather relevant details through information available in the public domain. Information will be sought from the Internet and other sources about the target Department, Internet services, connectivity and system configuration, network infrastructure, user management, access policies, etc. These activities explore the existence of security sensitive information on the public domain that is inadvertently or otherwise disclosed and may facilitate a hack attempt. The information gathered during this phase will be used to construct a theoretical schematic of the computing environment existing at the organization. This knowledge is used for carrying out the intrusive penetration testing

• **Level 2:** External Penetration Testing (Intrusive) on External Devices / Servers

External intrusive penetration testing will be carried out to simulate any attack from the Internet, identifying system weaknesses and exploiting them to gain access to the corporate network and other confidential resources. These activities are aimed at testing the security configuration of the IT systems enabling Internet connectivity and controls. Information gathered during the non-intrusive penetration tests will be exploited in this stage.

• **Level 3:** Internal Vulnerability Assessment (Non-Intrusive) on Internal Devices /Servers

An internal Vulnerability Assessment attempts to access the IT system from the internal network with no knowledge or limited prior knowledge of the computing environment which includes applications, database, operating systems and the networking technologies deployed.

• **Level 4:** Configuration Review for the network, equipment and computing environment

At this level the penetration testing team is equipped with additional information pertaining to the network and computing environment, which includes:

A manual configuration review is undertaken on identified network components (routers, switches, firewalls, VPN devices) and servers/ Operating Systems and Database configurations to determine misconfigurations.

At the end of this stage a detailed understanding of the IT architecture, application functionality and vulnerabilities that can be potentiality exploited will be documented

11.7.3 Penetration testing of Web Application

Web applications are increasingly becoming common targets for cyber attackers. Attackers tend to leverage simple web application vulnerabilities to gain access to confidential and personally identifiable information. Hence, it is essential that the government performs penetration testing of web applications to identify the vulnerabilities and take necessary measures.

Policy Statement

UT Administration of DNH and Daman & Diu shall perform penetration testing for web application by conducting below steps:

- User and application controls – Testing of user authentication failure responses; Lockouts and timeouts, username and passwords tests; Route messages to backend application and database servers; SQL injection
- Assess session controls - Validate cookie usage and settings; Exchange and alter session cookies; Alter URL and variable session information; Downgrade encryption settings
- Data, transaction analysis - Disrupt transaction integrity and send false transactions; Reuse transactions.

11.7.4 Application Security testing of web application

It is essential that the UT Administration of DNH and Daman & Diu performs application security testing of web applications to identify the vulnerabilities and take necessary measures.

Policy Statement

UT Administration of DNH and Daman & Diu shall perform application security testing for web application by conducting below steps:

- Structural analysis – Analyzing the structure of website which will involve identifying all pages; review of all user accessible HTML/source code; identify default, backup and inappropriate pages and testing the server platform; validation of headers and cookies etc.
- Input Validation - Validate controls for input and forms which will include input information of inappropriate length or type; input HTML or unprintable characters; attempt buffer overflow attacks; URL specific attacks

12. Operational Security

OPSEC is the process of denying hackers access to any information about the capabilities or intentions of a government by identifying, controlling and protecting evidence of the planning and execution of activities that are essential for the success of operations. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. The government shall treat OPSEC as a continuous process that consists of five distinct components:

- The UT Administration of DNH and Daman & Diu shall identify information that is critical to government.
- The UT Administration of DNH and Daman & Diu shall analyze the threat to that critical information.
- The UT Administration of DNH and Daman & Diu shall analyze the vulnerabilities to the government that would allow a cybercriminal to access critical information.
- The UT Administration of DNH and Daman & Diu shall assess the risk to government if the vulnerabilities are exploited.
- The UT Administration of DNH and Daman & Diu shall apply countermeasures to mitigate the risk factors.

The OPSEC components organize basic cybersecurity activities at their highest level. They help the government in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services. The subdivisions of OPSEC components results in outcomes closely tied to programmatic needs and particular activities of cyberspace. Examples include “Asset Management,” “Access Control,” and “Detection Processes.”

12.1 Cyber Plan Action Items

12.1.1 Identity of critical information

Identifying the information critical to the organization is essential. Based on the identification of critical information the government would be able to take appropriate decisions regarding the level of security that should be provided to protect this information.

Policy Statement

• The UT Administration of DNH and Daman & Diu will identify and manage data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes with their relative importance to government objectives and the organization's risk strategy.

• Examples of critical information include, but should not be limited to, the following:

- Citizen lists and contact information
- Contracts
- Patents and intellectual property
- Leases and deeds
- Policy manuals
- Articles
- Government papers
- Audio tapes
- Video tapes
- Photographs and slides
- Strategic plans and board meeting of minutes

12.1.2 Analysis of threats

A threat could be anything that leads to interruption, meddling or destruction of any valuable service or item existing in the department repertoire. Whether of human or nonhuman origin, the analysis must scrutinize each element that may bring about conceivable security risk.

Cyber threat analysis is a process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber-attacks.

Policy Statement

The government shall research and perform analysis to identify likely cyber criminals who may attempt to obtain critical information regarding the government operations. OPSEC planners should answer the following critical information questions:

- Who might be a cyber-criminal (e.g. Criminal, Terrorism, politically motivated hackers, etc.)?
- What are cyber criminal's goals?
- What actions might the cyber-criminal take?

- What critical information does the cyber-criminal already have on UT Administration of DNH and Daman & Diu operations? (i.e., what is already publicly available?)

12.1.3 Analysis of vulnerabilities

It is essential to identify the vulnerabilities of the government in protecting critical information. Examining each aspect of security that seeks to protect critical information and then comparing those indicators with the threats identified in the previous step.
Common vulnerabilities for government include the following:

- Poorly secured mobile/computer devices that have access to critical information.
- Lack of policy on what information and networked equipment can be taken home from work or taken out of state on travel.
- Storage of critical information on personal email accounts or other non-government networks.
- Lack of policy on what government information can be posted to or accessed by social network sites.

Policy Statement

The UT Administration of DNH and Daman & Diu will understand the cybersecurity risk to government operations (including mission, functions, image, or reputation), Government assets, and individuals. Outcome of this phase will be:

- Asset vulnerabilities are identified and documented
- Threats, both internal and external, are identified and documented
- Potential government impacts and likelihoods are identified
- Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- Risk responses are identified and prioritized

12.1.4 Assessment of risk

A cyber security risk assessment is necessary to identify the gaps in an government critical risk areas and to determine actions to close those gaps.

Policy Statement

The UT Administration of DNH and Daman & Diu OPSEC managers shall analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures to mitigate each one. Specific OPSEC measures must be selected for execution based upon a risk assessment done by government senior leadership. The government priorities, constraints, risk tolerances, and assumptions will be established and will be used to support cyber risk decisions

The Government Risk Management Strategy will involve below key steps:

- Risk management processes are established, managed, and agreed to by

all stakeholders

- Government risk tolerance is determined and clearly expressed
- The Government determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis

12.1.5 Application of appropriate OPSEC measures

It is essential for an organization to review and implement the OPSEC measures selected in the assessment of risk action. Before OPSEC measures can be selected, security objectives and critical information must be known, indicators identified and vulnerabilities assessed.

Policy Statement

The Government key OPSEC measures to mitigate risk will involve:

1 Access Control - Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

2 Awareness and Training - The government personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

3 Data Security - Information and records (data) are managed consistent with the government risk strategy to protect the confidentiality, integrity, and availability of information.

4 Information Protection Processes and Procedures – Government Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.

Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all -delivery channels in automated and online mode.

The government should notify the citizen, through alternate communication channels, of all Documentation process or fund transfer transactions above a specified value determined by the citizen

5. Maintenance - Maintenance and repairs of assets and information system components is performed consistent with policies and procedures.

13.Network Security

13.1 Internet Access

The internet connection is a channel from the outside world into the computer. If it is not secured properly someone may use it to access critical information or seize the connection or computer for their own purposes.

Policy Statement

- Access to and use of the internet from government premises must be secure and must not compromise information security of Government.
- Access to the Internet from government premises and systems must be routed through secure gateways. Any local connection directly to the Internet from Government premises or systems, including standalone PCs and laptops, is prohibited unless approved by Information Security. Employees shall be prohibited from establishing their own connection to the Internet using Government systems or premises.
- Use of locally attached modems with Government systems in order to establish a connection with the Internet or any third-party or public network via broadband, ISDN or PSTN services is prohibited unless specifically approved.
- Internet access provided by the Government must not be used to transact any commercial business activity that is not done by the Government.
- Personal business interests of staff or other personnel must not be conducted. Internet users are prohibited from transmitting, displaying or storing material that is fraudulent, obsessive, pornographic, profane, threatening, racially or sexually harassing or otherwise unlawful or improper or even visiting sites known to contain such material.
- Internet access provided by the Government must not be used to engage in any activity that knowingly contravenes any criminal or civil law or act. Any such activity will result in disciplinary action of the personnel involved.
- All applications and systems that require connections to the Internet or third-party and public networks must undergo a formal risk analysis during development and before production use and all required security mechanisms must be implemented.

13.2 Email Access

Email security refers to the measures used to secure the access and content of an email account or service. It allows an organization to protect the overall access to one or more email addresses/accounts. Failure to secure e-mail access may lead to serious security concerns.

Policy Statement

- Email System shall be used according to the Government policy.
- Access to email system shall only be obtained through official request.
- Email shall not be used to communicate confidential information to external parties unless encrypted using approved encryption facilities.
- Employees must consider the confidentiality and sensitivity of all email content, before forwarding email or replying to external parties.
- Information transmitted by email must not be defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation of the Government, or contain any material that is harmful to employees, citizens, politician, or others. The willful transmission of any such material is likely to result in disciplinary action.
- Government email system is principally provided for government purposes. Personal use of the Government email system is only allowed under management discretion and requires proper permission; such personal use may be withdrawn or restricted at any time.
- Government email address must not be used for any social networking, blogs, groups, forums, etc. unless having management approval.
- Rule based auto forwarding of emails from Government domain to public domain shall be restricted and not permitted.
- Email transmissions from the Government must have a disclaimer stating about confidentiality of the email content and asking intended recipient.
- Email management team at DC shall perform regular review and monitoring of email services.

13.3 Firewall Security

Firewall can serve as an efficient protecting tool for an organization's system. It prevents unauthorized access to the organization's network. It will automatically refuse and decrypt the unwanted information through the network. It can help save the organization's data from the hackers.

Policy Statement

- Guidelines shall be followed to ensure protection of government systems by monitoring and controlling incoming and outgoing traffic using firewalls.
- Configuration backups and logs shall be retained as per statutory and regulatory requirements.
- The government shall use a robust "Firewall System" interposed between the Internet and the government private network.
- All Internet traffic from inside to outside, and vice-versa, must pass through the firewall implementation.
- Access from the Internet to the government public information systems must not make sensitive information or information systems vulnerable to compromise.
- Only network sessions using strong authentication and encryption will be permitted to pass from the Internet to inside through the firewall

implementation.

- Where users are required to access internal systems and networks from, or across, the Internet, end-to-end encryption and strong authentication controlled by a department will be employed.
- The firewall shall be configured to deny all services not expressly permitted and will be regularly audited and monitored to detect intrusions or misuse. The firewall will notify the firewall administrator(s) in near-real-time of any item that may need immediate attention such as a break-in into the network, little disk space available, or other related messages so that an immediate action could be taken.
- If the firewall software is run on a dedicated computer - all non-firewall related software, such as compilers, editors, communications software, etc., will be deleted or disabled.
- After a failure, all firewalls will fail to a configuration that denies all services, and require a firewall administrator(s) to re-enable services. Source routing will be disabled on all firewalls and external routers. The firewall will not accept traffic on its external interfaces that appear to be coming from internal network addresses.
- The firewall will provide detailed audit logs of all sessions so that these logs can be reviewed for any anomalies.
- Secure media will be used to store log reports such that access to this media is restricted to only authorized personnel.
- Firewalls will be tested off-line and the proper configuration verified.
- The firewall will be configured to implement transparency for all outbound services. Unless approved by the government, all in-bound services will be intercepted and processed by the firewall.
- Appropriate firewall documentation will be maintained on off-line storage at all times. Such information will include but not be limited to the network diagram, including all IP addresses of all network devices, the IP addresses of relevant hosts of the Internet Service Provider (ISP) such as external server, router, DNS server, etc. and all other configuration parameters such as packet filter rules, etc. Such documentation will be updated any time the firewall configuration is changed. The government shall review the firewall configuration settings during the course of audit.
- Where requirements for network connections and services have changed, the security policy will be updated and approved.
- The firewall implementation (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files should be locked up so that the media is only accessible to the appropriate personnel.
- Only the firewall administrator(s) will have privileges for updating system executables or other system software. Any modification of the firewall component software must be done by a firewall administrator(s) and requires the formal approval via **change request process**.
- The firewall administrator(s) must evaluate each new release of the firewall software to determine if an upgrade is required.

- All security patches recommended by the firewall vendor should be implemented in a timely manner. For getting updates for patch and updates from OEMs the Government may choose to be a part of the mailing list of the OEMs.
- All services and traffic to be authorized across the firewall implementation must be well documented. Documented will be the government need, protocol used, inbound and/or outbound, port assignments, known vulnerabilities, and risk mitigation statements.
- If application-level proxy firewalls are used, out-bound network traffic should appear as if the traffic had originated from the firewall (i.e. only the firewall is visible to outside networks).

13.4 Logging of Network Devices

Logging of Network devices in the organization can help detect unusual network traffic or network device failures. Hence, it is important to implement logging to get insight into all activities happening in the organization's network.

Policy Statement

Event logs from the routers, switches and firewalls shall be stored on a server for a period as prescribed by statutory and regulatory authorities, with restricted access and monthly review.

13.5 Network Monitoring

Network monitoring is essential to detect hacking attempts, virus or worm infections and propagation, configuration problems, exploits, hardware problems and many others. Monitoring is also an important factor to maintain stability for the network.

Policy Statement

- UT Administration of DNH and Daman & Diu shall prepare and maintain an up-to-date network architecture diagram at the organization level including wired/wireless networks
- Maintain an up-to-date/centralized inventory of authorized devices connected to government's network (within/outside government's premises) and authorized devices enabling the government's network.
- All critical network devices such as routers, switches and firewalls shall be proactively monitored and breach incidents will be logged by the operational personnel.
- The Government shall establish appropriate security monitoring systems and processes, to facilitate prompt detection of unauthorized or malicious activities by internal and external parties.
- The Government shall implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect the Government against network intrusion attacks as well as provide alerts when an intrusion

occurs.

- The Government may implement security monitoring tools which enable the detection of changes to critical ICT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes.
- The Government shall regularly review security logs of systems, applications and network devices for anomalies. Logs shall be protected and retained for defined period to facilitate future investigation.

13.6 Dynamic Host Configuration Protocol

DHCP provides automatic and reliable TCP/IP network configuration, and ensures that address conflicts do not occur.

Policy Statement

The government shall implement a DHCP (Dynamic Host Configuration Protocol) to ensure that only authorized machines are accessing the government's network and have access to the company's IT resources.

13.7 Remote Access – Virtual Private Network

VPNs, or Virtual Private Networks, allow users to securely access a private network **and** share data remotely through public networks.

Policy **Statement**

- Any connection between firewalls over public networks will use encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network.
- All connections between clients to services or applications located behind the firewall within government's trusted network, that are over untrusted public networks will use encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network. Such connections will be considered extensions of government's trusted network, and as such will not fall under the service restrictions that follow. Access to VPN shall be provided to employees/visitors/contractors based on the request initiation and approval by authorized personnel. Periodic reconciliation of access shall be performed. End users shall be given appropriate training on usage of VPN and security precautions.

13.8. Wireless Access

Using a wireless network in gives a lot of convenience to an organization. However, if the wireless network is not secure, there are significant risks.

Policy Statement

The UT Administration of DNH and Daman & Diu shall ensure that wireless access to the network is configured such that authorized employees are authenticated prior to gaining access. All wireless infrastructure devices that reside at a government site and connect to a government network, or provide access to information classified as government Confidential, or above must:

- Abide by the standards specified in the Wireless Communication Standard.
- Be installed, supported, and maintained by an approved support team.
- Use government approved authentication protocols and infrastructure.
- Use government approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

All employees, contractors, consultants, temporary and other workers at the government, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the government must adhere to this policy.

This policy applies to all wireless infrastructure devices that connect to a government network or reside on a government site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

13.8 Patch Management for Network Devices

The threat of malicious virus and worm attacks has been increasing thus forcing government to reinvestigate their security needs to better protect their environment. Research has shown that the most efficient way to be protected against attacks is to ensure that every network device has the latest patches installed. Hence, it is imperative that the organization has an efficient patch management process in place.

Policy Statement

- The Government shall establish and ensure that the patch management procedures include identification, categorization and prioritization of security patches.
- To implement security patches in a timely manner, the Government shall establish the implementation timeframe for each category of security patches. The Government shall perform rigorous testing of security patches before deployment into the production environment.

13.9 Change Management

Implementation of an efficient change management process is essential in an organization. Lack of proper change management process may lead to the following risks:

- unauthorized changes may take place
- application owner/other stakeholders are unaware of the change
- list of changes to an application/software cannot be tracked
- multiple versions of an application may exist is appropriate change control is not followed
- in case changes are not reviewed and analyzed before implementation, potential risks/damage to the environment will not be known
- no backout plan if the changes implementation fails

Policy Statement

Any configuration changes to the government's network infrastructure and associated security devices shall follow the Change Management procedure. Refer Change Management Procedure for details on the change management procedure.

13.10 Clock Synchronization

The synchronization of time on all network devices is very important. In its absence the time on individual network device may slowly drift away from each other at varying degrees until potentially each has a significantly different time.

Policy Statement

The government shall ensure that clocks for all network devices would be synchronized through the global NTP server.

13.11 Enforcement

The cyber security policy is effectively useless unless it is enforced. Effective enforcement is necessary to ensure that all employees are aware of the risks and consequences of noncompliance.

Policy Statement

Any employee, contractor or third party found to have violated this policy may be subjected to disciplinary action, including termination of employment/contract. Appropriate legal action may be taken to recover damage caused by the violation.

13.12 Sustenance

It is important that there is continuous improvement and sustenance of the network security in an organization.

Policy Statement

Periodic reviews will be performed in order to ensure continuous improvement and

sustenance of the Network Security, as listed in the procedure. The Government shall conduct VAs regularly to detect security vulnerabilities in the ICT environment. The Government shall deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based systems, the scope of VA shall include common web vulnerabilities such as SQL injection, cross-site scripting, etc. The Government shall establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed. The Government shall carry out penetration tests in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. The Government shall conduct penetration tests on network infrastructure and internet-based systems periodically or need basis.

14. Communication Management

Exchange of information between the government and other organizations shall be protected by adequate controls and the communication resources shall be used for business purposes only.

14.1 Encryption

14.1.1 Use of Encryption

The main aim of encryption is to protect the confidentiality of data stored on computer systems or transmitted via the internet or other computer networks. Without encryption there is a risk of confidential data being intercepted and used by unauthorized personnel.

Policy Statement

- Cryptographic controls like encryption shall be implemented to protect the confidentiality of sensitive information when being transmitted and/or stored on the government's information resources. Encryption is recommended for transmission over network links containing equipment that is not owned or controlled by the government as well.
- Based on the risk assessment, where ever required, cryptographic controls shall be used to achieve different security objectives, e.g.:
    - confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
    - integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;
    - Non-repudiation: using cryptographic techniques to obtain proof of the occurrence or nonoccurrence of an event or action.
- While implementing cryptographic controls, consideration shall be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of

trans-border flow of encrypted information. Legal and Compliance shall be consulted for the proposed use of restricted encryption products for deployment outside India.

- Specialist advice shall be sought to identify the appropriate level of protection and to define suitable specifications that will provide the required protection and support the implementation of a secure key management system.
- Government personnel, third party consultants, contractors and vendors shall not implement encryption, digital signatures, digital certificates or key escrow mechanisms for the government's process without prior authorization from Information Security Team.
- Digital signature certificates shall be used to authenticate the identity of individuals when Confidential or Restricted government information is being externally accessed via the Internet.
- Legal and Compliance shall handle all legal requests for access to encryption keys in the event encrypted information is needed in unencrypted form as evidence in a court case.
- Authentication and network/transport layer encryption shall be used for Wireless connections to protect wireless access to the information system.
- When cryptography is employed within the information system, the system shall perform all cryptographic operations (including key generation) using validated cryptographic modules operating in approved modes of operation.

14.1.2 Digital Signatures

A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.

Policy Statement

- Digital signatures shall be used when there is a legal, contractual or business need to verify the author or integrity of a document. Digital signatures shall always be used when sending or receiving personally identifiable information of citizens or employees.
- For the issuance of digital signatures, branch personnel shall contact the Head Office IT department with proper application and supporting document. Head Office IT department shall ensure that the required procedures are followed.
- Government shall also consider use of "digital signatures" in identified information exchanges – to ensure authenticity and integrity. Such usage depends upon business needs. This may also be considered where "non-repudiation by either party" is to be ensured.
- Non-repudiation services shall be used to resolve dispute between parties, regarding the occurrence or non-occurrence of an event or action involving the use of digital signatures or any associated encryption protocol.
- No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—

a) The Certifying Authority listed in the certificate has not issued it; or
b) The subscriber listed in the certificate has not accepted it; or
c) The certificate has been revoked or suspended,

Unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

Users shall ensure that digital signature issued by the Government should be used for Government's official purposes only. On loss of certificate, users shall abide by the standard procedure laid down by the government and should approach HO IT department for immediate resolution.

14.1.3 Key Management

Encryption key management is vital to securing enterprise data storage and the organization should ensure that there is an effective Key Management process in place.

Policy Statement

- All encryption processes running on the government's information resources (e.g., email and/or any application using encryption services) shall include centralized key recovery functions, which may only be accessed by authorized personnel.
- All cryptographic keys shall be protected against modification, loss, and destruction.
- Encryption key owners are responsible for the protection and management of public and private encryption keys entrusted to them.
- Secret and private keys shall be protected against unauthorized disclosure.
- Equipment used to generate, store and archive keys shall be physically protected.
- When required by law, encryption keys used for encryption of stored data shall be backed up or escrowed to ensure availability in case the original key is lost or corrupted.
- To protect against potential compromise, encryption keys shall expire and be renewed periodically. If the keys are compromised or suspected to be compromised, they shall be changed & updated.

14.2 Information Exchange Agreements

It is essential for an organization to have documented information exchange agreements (NDA – Non disclosure agreement), in the absence of which there could be a risk of sensitive information being inappropriately handled by an external party.

Policy Statement

- Formal information exchange agreements shall be executed when exchanging information between the government and external organizations, based on the sensitivity of the information involved.

- Exchange Agreement shall clearly state how external organization should deal with secrecy of information should be maintained and also state how information n should be destroyed after its intended use
- Government shall add penalty clauses to exchange agreement to enforce the external organization to abide by the agreement

14.3 Publicly Available Information.

Adequate care should be taken to protect the integrity of electronically published information to prevent unauthorized modification, which could harm the reputation of the Government.

Policy Statement

- The web publishing duties shall be separated by having a designated author for content creation & edition and an approver to sign-off on the changes.
- Authors shall have publishing responsibility and necessary training, which is recognized by their line manager/supervisor. Content approvers shall be assigned by the Head of a government unit, have the authority and desire to take responsibility of the published content and have the appropriate level of knowledge regarding legal responsibilities and risks of publishing public information.
- The sections of the Website that carry classified matter shall authenticate users through passwords and other mechanisms before allowing access.
- Websites shall not contain any matter that is confidential or the leakage of which would jeopardize the interests of the government and its related parties.

14.4 Email, Internet and Other Electronic Communication.

14.4.1 Business Use.

Information resources and other systems used to generate, receive and store electronic communications are property of the organization. Improper use of any of these resources or systems can result in leakage of critical information.

Policy Statement

All personnel are required to conduct themselves in a professional manner, reflecting the government's high ethical standards in all of their communications. Government personnel are prohibited from engaging in the following electronic mail practices:

- Mass transmission of unwanted electronic mail messages (spamming)
- Retransmission of chain messages
- Spoofing the identity of another user

Electronic mail and any other electronic systems provided by the government are provided for its business use only. Any other use, except for reasonable and

occasional personal use, is prohibited. The use of external personal email while connected to the government's network is prohibited.

Any data/files/information residing on the Government Information systems, including the same received and sent through government email system, is owned by the Government. All users must be made aware that government has full rights to view/use/delete/control such information.

14.4.2 Use of Encryption

It is important for the organization to ensure appropriate use of encryption. Failure to do so might result in serious compromise of critical information.

Policy Statement

Information classified as Confidential or Restricted shall not be sent over the Internet (e.g., email, ftp), via Remote Access or other external networks unless the message is using an encryption service approved by the Information Security Team.

14.4.3 Acceptable Use

Without guidelines on acceptable use of the organization's resource and information, the employees would be unaware of how to handle sensitive information.

Policy Statement

All electronic communications shall be prepared with the same care and professionalism as letters, memoranda or other written communications that bear the government's logo. The use of inappropriate language in any electronic communication is prohibited, including the transmission and re-transmission of electronic mail containing illegal, slanderous, libellous, defamatory, abusive, derogatory, threatening, obscene, racist, sexist or otherwise offensive materials.

14.4.4 Retention / Deletion of Electronic Mails

In order for the organization to function administratively, undergo periodic audits and provide for its legal requirements, it must manage its records properly. Therefore, the organization requires its employees to retain and destroy e-mail messages that are sent and received in the course of conducting official business in accordance with an approved company policy.

Policy Statement

- The Government's email management team at DC shall ensure that electronic mail data is periodically backed up and stored offsite. Electronic mail users shall be made aware that electronic mail messages are periodically backed up and that messages, although deleted from a user's electronic mail file, still exist until the backup medium is erased.

- While electronic mail messages are periodically backed up, the government does not guarantee the long-term storage of electronic mail messages. Employees shall take the appropriate steps to store the contents of electronic mail to the appropriate media in order to satisfy legal and regulatory retention requirements.
- Electronic mail systems are not intended for the archival storage of important business information. Electronic mail messages shall only be retained as long as they are necessary for conducting business. Information sent or received by electronic mail shall be moved to appropriate media to satisfy legal and regulatory retention requirements.
- Electronic mail restoration request by employees shall be approved by Legal & Compliance before the request is processed.

14.4.5 Personal Websites

It is imperative that the organization's resources are not utilized by any personnel for personal use. In such case there is a risk of damage to the government name as well as compromise of critical information in certain cases.

Policy Statement

- Government personnel, third party consultants, contractors and vendors shall not publish personal Web sites on government owned or leased information resources. In addition, using the brand name (UT Administration of DNH and Daman & Diu.) or conducting the government's business in any form on the Internet, including creating a Web site, Web page or domain on the Internet is strictly forbidden.

14.4.6 Social and Professional Networking Media

In case of inappropriate use of social media and professional networking sites there is a risk of leakage of sensitive and critical information.

Policy Statement

- Government personnel, third party consultants, contractors and vendors shall not publish any sensitive/ confidential information about the government, its strategies, trade secrets and Projects in the internet message boards, bulletin boards, blogs, social or professional networking websites.

14.5 Voice, Fax and Video Communications

Information resources and other systems used to generate, receive and store voice, fax and video communications are property of the organization. Improper use of any of these resources or systems can result in leakage of critical information.

Policy Statement

- All government employees are required to conduct themselves in a professional manner, reflecting its high ethical standards, in all of their communications.
- Phone calls, voice mail, faxes, teleconference and any other voice communication systems provided by the government are provided for use in connection with its business. Any other use, except for reasonable and occasional personal use, is prohibited.

14.5.1 Acceptable Use

Without guidelines on acceptable use of the organization's resource and information, the employees would be unaware of how to handle sensitive information.

Policy Statement

- All voice, fax and video communications shall reflect the core values, policies and ethics of the government. The use of inappropriate language in any voice, fax or video communication is prohibited, including illegal, slanderous, libellous, defamatory, abusive, derogatory, threatening, obscene, racist, sexist or otherwise offensive materials.

14.5.2 Phone Calls

Due of the malice of social engineering, phone calls and voice mails have become a device for hackers to gather sensitive information about an organization. Hence, it is essential that employees are made aware of the risks.

Policy Statement

- When making or receiving a telephone call, personnel are responsible for the confidentiality of their conversation. If Confidential or Restricted information needs to be discussed, the identity of the receiving party shall be verified.
- The government shall implement usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously.

14.5.3 Voice Mails

Due to the malice of social engineering, phone calls and voice mails have become a device for hackers to gather sensitive information about an organization. Hence, it is essential that employees are made aware of the risks.

Policy Statement

- Voice messages shall be left/ reviewed in a manner which is responsible for the confidentiality of the information being left/ reviewed.

14.5.4 Facsimile

When making copies of any critical information, it is essential that proper precaution is taken to ensure that there is no leakage of information.

Policy Statement

- When sending or receiving a fax, personnel are responsible for the confidentiality of the information transmitted.

14.5.5 Conference Calls / Video Teleconferences.

When participating in conference calls and video teleconferences, personnel are responsible for the confidentiality of their conversation. Precaution should be taken to ensure that no critical or sensitive information is shared with any unauthorized personnel.

Policy Statement

- Information systems shall prohibit remote activation of collaborative computing mechanisms (e.g., video and audio conferences) and provide an explicit indication of use to local users (e.g., use of camera or microphone). Video conferencing information systems shall also provide physical disconnect of camera and microphone in a manner that supports ease of use.

- Video conferencing encryption is required to ensure confidentiality during online meetings, seminars and negotiations. Even if an intruder succeeds in intercepting the video stream, he will not be able to decrypt it.

14.6 Meetings & Conversations

14.6.1 Conference Calls / Video Teleconferences

When participating in conference calls and video teleconferences, personnel are responsible for the confidentiality of their conversation. Precaution should be taken to ensure that no critical or sensitive information is shared with any unauthorized personnel.

Policy Statement

- Non-disclosure forms, as necessary, shall be obtained while disclosing sensitive information.

14.6.2 Public Conversations

When conversing in public, personnel are responsible for the confidentiality of their conversations. Social engineers can extract critical information in such scenarios.

Policy Statement

- Government personnel shall avoid discussing with their family and friends any topic about their work that could lead to disclosing its sensitive information. During travel, personnel shall be alert for indications that fellow travellers or new acquaintances are interested in their business affairs.

15. Incident Management.

An incident is any activity that causes real or potential adverse impact on data, systems, networks or organization due to unauthorized or malicious use of the resources. **Incident** is a term related to exceptional situations or a situation that warrants intervention of security administrators/senior management.

Some examples of Information Security Incidents are:

- hacking attempts
- Email spoofing
- Denial of Service
- Loss of information due to unknown reasons
- Virus incidents regarding e-mail, Internet, CD, diskette and others
- Power problems and loss of data
- Hardware, Software, and Operational errors that results in erroneous data
- Use of unauthorized software
- Tail gating
- Sharing of confidential or unauthorized information to unintended users / everyone
- Violation of security policies

To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Policy Statement

- All employees and service providers must be made aware of controls on information system security incidents such as computer frauds, malicious codes, viruses and worms, network penetration and other attacks, malfunction of software and security weaknesses and must be made aware about their responsibility in this respect.
- Users shall be prohibited from possessing software or other tools that are designed to compromise information security.
- Employees shall remain vigilant for possible fraudulent activities or occurrence of security incidents.

15.1 Reporting Security Weaknesses

Government shall ensure that all employees, contractors and third-party users of information systems and services are required to note and report any observed or suspected cyber security weaknesses.

Policy Statement

- All employees, contractors and third-party users of information systems and services shall notify immediately of all identified or suspected Cyber Security weaknesses to the Chief Information Security Officer (CISO). There may be times, when in order to comply with legal requirements or regulations, cyber security incidents must be reported to outside authorities. This should only be done by authorized persons.
- Information Security incidents shall be reported to Chief Information Security Officer (CISO) by sending an email or reporting it on Government intranet under information security incident/weakness reporting section. In case of any critical incident, needing immediate attention shall be reported over CISO's mobile number (published) which shall be followed by email notification.
- CISO shall investigate into the incident and take necessary preventive and corrective actions and if required, initiate disciplinary action process.
- In Compliance with RBI guidelines Government shall participate in the activities of their CISOs' Forum coordinated by MeitY and promptly report the incidents to Indian Governments – Centre for Analysis of Risks and Threats.
- Government shall report each incident within 6 hours of its occurrence to CISO.
- Government shall also report major security incidents to CERT-In, and Law enforcement agencies whenever is required.

Please refer to "Government's Cyber Crisis Management Plan" for detailed guidance on Cyber Incident Reporting.

15.2 Cyber Security Operation Centre (C-SOC)

It is to be noted that the threat landscape has changed significantly in the recent past and therefore the approach and methodology required to be put in place has to necessarily take into account proactive approaches rather than reactive approaches and have to also address possible unknown attacks. For example, zero-day attacks and attacks for which signatures are not available have to be kept in mind. The Cyber SoC has to take into account proactive monitoring and management capabilities with sophisticated tools for detection, quick response and backed by data and tools for sound analytics.

Policy Statement

- The SOC shall take into account collection of the logs from each one of the point products deployed, storing and processing of the logs, correlation through appropriate SIEM tools, continuous monitoring of SIEM screens and finding the anomalies, if any and raising the alarms.
- The SOC shall identify root cause of attacks, classify them into identified categories and come out with solutions to contain further attacks of similar types.
- The SOC shall be able to conduct Dynamic Behavior Analysis. – Preliminary static & dynamic analysis and collecting Indicators of Compromise (IOC). Some examples of key indicator of compromise to be monitored are:
    - Unusual outbound network traffic
    - Anomalies in privileged user account activity
    - geographical irregularities in log-ins and access patterns
    - Log-in irregularities and failures
    - spike in database read volume
    - larger HTML response size than a normal request
    - Large Numbers of Requests for The Same File
    - Mismatched Port-Application Traffic
    - Suspicious Registry or System File Changes
    - DNS Request Anomalies
    - Unexpected Patching of Systems
    - Mobile Device Profile Changes
    - Bundles Of Data in The Wrong Places
    - Web traffic that doesn't match up with normal human behavior
    - Signs Of DDoS Activity
- The SOC shall have the capacity to monitor logs in real time/near real time.
- The SOC shall be equipped with good analytics dash board, showing the Geolocation of the IP's
- The UT Administration shall ensure monitoring of SOC on 24*7 basis. the staff within the SOC must have the appropriate tools, diagrams, and knowledge of the network to perform their daily job
- Shift logs must be maintained for audit and to ensure continuity of the SOC operations. SOC shift logs should be maintained daily for every shift.
- The SOC manager shall review all incident records regularly to ensure they were resolved within the parameters of the defined severity levels. The manager shall also audit incident records that have exceeded standard resolution times to validate that the incident records were handled appropriately.
- The government shall integrate SOC with various threat intelligence feeds from external sources like other governments, financial ecosystem, Cyber response cells, CERT-In, telecom service providers etc.

15.3 Responding to Information Security Incidents and Weaknesses

The Chief Information Security Officer (CISO) shall respond timely, effectively and orderly to all Cyber Security incidents, liaison and coordinate with appropriate personnel to gather information and offer advice.

Policy Statement

- Government shall have a formal Incident Response programme which is approved by the Board/Top Management.
- Government shall define and document, Incident response procedures, including the roles of staff / outsourced staff handling such incidents.
- Government shall design response strategies to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication & coordination with stakeholders during the response.
- Government shall have process in place to incorporate the lessons learnt in order to continually improve the response strategies.

15.4 Management of Information Security Incidents & Improvements

Not having an effective information security incident management plan may lead to incidents not being reported and addressed in time, loss of confidentiality, integrity and/or availability of data, loss of reputation for the government, disruption of services as well as legal & compliance issues.

Policy Statement

- The Government shall establish an incident management framework with the objective of restoring normal technology-based service as quickly as possible following the incident with minimal impact to the government operations.
- The Government shall also establish roles and responsibilities of staff involved in the incident management process, which includes recording, analyzing, remediating and monitoring incidents.
- The Government shall accord incidents with the appropriate severity level. As part of incident analysis, the Government may delegate the function of determining and assigning incident severity levels to a technical helpdesk function. The Government shall train helpdesk staff to determine incidents of high severity level. In addition, criteria used for assessing severity levels of incidents shall be established and documented.
- The Government shall establish corresponding escalation and resolution procedures where the resolution timeframe is proportionate with the severity level of the incident. The predetermined escalation and response plan for security incidents shall be tested on a periodic basis.
- The Government shall form a Cyber Incident Response Team, comprising staff within the Government with necessary technical and operational skills to

handle major incidents.

- In some situations, major incidents may further develop adversely into a crisis. Senior management shall be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made on a timely basis as defined in the business continuity and disaster recovery plan.
- The Government shall keep citizens informed of any major incident. Being able to maintain citizen confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of the Government.
- Government shall periodically test the effectiveness of the Incident response plan
- As incidents may trail from numerous factors, Government shall perform a root-cause and impact analysis for major incidents which result in severe disruption of cyber services. The Government shall take remediation actions to prevent the recurrence of similar incidents.
- The root-cause and impact analysis report shall cover following areas:
  - Root Cause Analysis
    - When did it happen?
    - Where did it happen?
    - Why and how did the incident happen?
    - How often had a similar incident occurred over last 2 years?
    - What lessons were learnt from this incident?
  - Impact Analysis
    - Extent of the incident including information on the systems, resources, citizens that were affected;
    - Magnitude of the incident including foregone revenue, losses, costs, investments, number of citizens affected, implications, consequences to reputation and confidence;
    - Breach of regulatory requirements and conditions as a result of the incident.
  - Corrective and Preventive Measures
    - Immediate corrective action to be taken to address consequences of the incident. Priority shall be placed on addressing citizens' concerns.
    - The Government shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

15.5 Remedies to Information Security Incidents and Weaknesses

The organization should have a strategy in place to address any information security incident within an appropriate timeframe. Failure to do so might result in loss of critical information and the organization's reputation.

Policy Statement

- Government shall explore response strategies to meet various incident

scenarios based on situational awareness and potential/post impact, consistent communication & coordination with stakeholders during the response.

- A list or catalog of Cyber Security, threats and 'remedies' may be planned by the Government which may be studied regularly with the anecdotal evidence used to aid in the reduction of risk and frequency of Information Security incidents in the organization.
- Government may establish and implement systems to collect and share threat information from local/national/ international sources following legally accepted/defined means/process.
- Government may implement a policy & framework for aligning Security Operation Centre, Incident Response and root cause analysis to reduce the business downtime/ to bounce back to normalcy.
- Government shall have process in place to incorporate the lessons learnt in order to continually improve the response strategies.

15.6 Monitoring Confidentialities for Information Security Incidents

There is a risk of advertent/ inadvertent leakage of critical information if case of releasing information regarding the information security incident.

Policy Statement

- Only authorized personnel may release information relating to Cyber Security incidents.

15.7 Collection of Evidence of Information Security Incidents

Collection of Evidence of Information Security Incidents is essential to analyze the nature of the incident and to ensure that mechanisms are devised to prevent the reoccurrence of such incidents.

Policy Statement

- Evidence of a Cyber Security breach must be properly collected, retained, and presented to the Chief Information Security Officer (CISO). The evidence collection, retention and presentation shall conform to the rules for evidence laid down in the jurisdiction of the government's operations.
- Government shall periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, MeitY, NIC etc.
- Please refer to "Government's Cyber Crisis Management Policy" for detailed procedure of Forensic Analysis.

15.8 Ensuring the Integrity of Information Security Incident Investigations

The organization is responsible for ensuring the integrity of information security incident investigations. Failure to do so might result in reoccurrence of similar security incident and a negative impact on the UT Administration of DNH and Daman

& Diu name.

Policy Statement

- Information systems and computing device use must be monitored regularly with all unforeseen events recorded and investigated. The Information systems must be audited from time to time with the combined results and history strengthening the integrity of any subsequent investigations.
- The Government shall adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

16. Problem Management

While the objective of incident management is to restore the information and communication technologies service as soon as possible, the aim of problem management is to determine and eliminate the root cause to prevent the occurrence of repeated incidents.

Policy Statement

- Government shall establish a process to log the information system related problems.
- The Government shall have the process of workflow to escalate any problem to a concerned person to get a quick, effective and orderly response.
- Problem findings and action steps taken during the problem resolution process shall be documented.
- A trend analysis of past problems shall be performed to facilitate the identification and prevention of similar problems.

17. Capacity Management

The goal of capacity management is to ensure that information and communication technologies capacity meets current and future government requirements in a cost-effective manner.

Policy Statement

- To ensure that systems and infrastructure are able to support government functions, the Government shall ensure that indicators such as performance, capacity and utilization are monitored and reviewed.
- The Government shall establish monitoring processes and implement appropriate thresholds to plan and determine additional resources to meet operational and government requirements effectively.

18. Access Management

The Government shall only grant access rights and system privileges based on job responsibility. The Government shall check that no person by virtue of rank or position shall have any intrinsic right to access confidential data, applications, system resources or facilities for legitimate purposes.

The access control policy shall be reviewed periodically based on government service and security requirements.

18.1 Business requirement for Access control

Government shall ensure that sound and strict access controls are established to prevent unauthorized access to information and information systems.

Policy Statement

- The policy adopts “closed access control policy” i.e. access is denied to all for all operations for all Information resources unless it is required for need-to-do and it is explicitly given.
- Access shall be controlled on the basis of information classification. These policies are applicable for all logical accesses to all information systems.
- The owner of the system must authorize access to all systems and the appropriate access rights must be recorded in an access control list.
- Third party users permitted to access government internal systems via real-time computer connections (dial-up lines, the Internet, value added networks, etc.) shall have specific approval of the IT Department. Access privileges for third party users shall be enabled only for the time required to accomplish previously defined and approved tasks.

18.2 User Registration and De-Registration

Government shall ensure that there is formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

Policy Statement

- Logical access shall be granted to the government employees, third party staff and external parties by requiring compulsory user registration for all users, who are authenticated by use of quality passwords and have access rights based upon “need to do and need to know basis” also taking into consideration need for dual control of maker-checker controls.
- Access shall be restricted according to the user’s requirement to read, write, execute or delete information, data or software based on business requirements.

- Access shall be granted only on allowed information asset by the request or based on the needs of the business and the level of information security required.
- User login ids must be identifiable, unique.
- The Government shall closely monitor non-employees (contractual, outsourced, or vendor staff) for access restrictions.
- User access privileges must be kept updated for job status changes.
- Multiple, generic, default ids shall be replaced with named user ID's.
- User access to systems shall be revoked as part of the "Exit Formality" that is followed when an employee leaves the organization.
- IT must perform a periodic reconciliation of the active user IDs with the active employee's data. The concerned departments will review and verify that access to government systems by an employee who is no longer working with the organization is duly removed.

18.3 Privileged Access Management

Government shall ensure that the allocation and use of privileges is restricted and controlled.

Policy Statement

- Information security ultimately relies on trusting a small group of skilled staff, who shall be subject to proper checks and balances. Their duties and access to systems resources shall be placed under close scrutiny.
- The allocation of privileges shall be controlled through a formal authorization process to protect multi-user systems against unauthorized access.
- The Government shall apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions.
- Having privileged access, all system administrators, programmers and employees performing critical operations invariably possess the capability to inflict severe damage on critical systems. The Government shall adopt following controls and security practices for privileged users:
    - Implement strong authentication mechanisms;
    - Implement strong controls over remote access;
    - Restrict the number of privileged users;
    - Grant privileged access on a "need-to-have" basis;
    - Review privileged users' activities on a timely basis;
    - Prohibit sharing of privileged accounts;
    - Disallow vendors from gaining privileged access to systems without close supervision and monitoring;

18.4 Input Control

All input controls including session time-out periods, audit trails, etc., need to be defined and implemented to ensure safekeeping of all sensitive and critical

information.

Policy Statement

- Session time-out period for users shall be set in accordance with the Government's existing practice.
- Operating time schedule of users' input for government applications shall be implemented as per regulatory enforcement unless otherwise permitted from appropriate authority.
- Audit trail with User ID and date-time stamp shall be maintained for data insertion, deletion and modification.
- Software shall not allow the same user to be both maker and checker of the same application unless otherwise permitted from appropriate authority.
- Management approval must be in place for delegation of authority.
- Sensitive data and fields of government applications shall be restricted from being accessed.

18.5 User Responsibilities

It is essential that all Government personnel are made aware of the user responsibilities to combat cyber risks.

Policy Statement

- Government shall ensure to prevent unauthorized access to information and information systems, unauthorized user access, and compromise or theft of information and information processing facilities.

18.5.1 Password Use or management

Government shall ensure that Users are required to follow good security practices in the selection and use of passwords. A strong password is a key defense against any attempt to compromise the logical security of computer systems. Weak passwords increase the vulnerability of computer systems to brute force and/or dictionary attack.

Policy Statement

- The government employees shall create passwords in line with the complexity rules as defined in the Access Control Procedure defined by the government.
- Password controls shall include a change of password upon first logon
- All government employees, third party staff and external parties shall be advised to:
  - keep passwords confidential;
  - avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;

- change passwords whenever there is any indication of possible system or password compromise;
- select quality passwords with sufficient minimum length which are:
  - easy to remember;
  - Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, phone numbers, and dates of birth etc.
  - not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
  - free of consecutive identical, all-numeric or all-alphabetic characters;
- change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;
- change temporary passwords at the first log-on;
- not include passwords in any automated log-on process, e.g. stored in a macro or function key;
- not share individual user passwords;
- not to use the same password for government and non-government purposes

- If users need to access multiple services, systems or platforms, and are required to maintain multiple separate passwords, they shall be advised that they may use a single, quality password for all services where the user is assured that a reasonable level of protection has been established for the storage of the password within each service, system or platform.
- IT department shall take special care for management of the help desk system dealing with lost or forgotten passwords as this may also be a means of attack to the password system.
- Government shall ensure the complexity of password by setting various parameters like Password History, Maximum password age, Minimum password length, Password lockout duration, account lockout threshold etc.

18.5.2 Unattended user equipment

Users must ensure that unattended equipment has appropriate protection. Failure to do so might result is compromise of data stored in such equipment.

Policy Statement

Personal computers and computer terminals and printers shall not be left logged on when unattended and shall be protected by key locks, passwords or other controls when not in use.

18.5.3 Clear desk and clear screen Policy

- Government shall ensure that a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted.

Policy Statement

- No important information asset of the government shall be left out on desks after working hours.
- Personal computers and computing terminals shall be attended to when in 'logged on' condition & shall be protected with screen saver passwords and automatic account logout times, wherever possible.
- Where appropriate, paper and computer media shall be stored in suitable locked cabinets and / or other forms of security furniture when not in use, especially after working hours.
- Sensitive or critical information shall be locked away (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.
- Personal computers and computer terminals and printers shall not be left logged on when unattended and shall be protected by key locks, passwords or other controls when not in use.
- Unattended fax machines shall be protected.
- Photocopiers shall be protected from unauthorized use especially after normal working hours.

18.6 Review of User Access Rights

The purpose of reviewing user access control is to help ensure the protection of the government data from accidental or intentional unauthorized access

Policy Statement

- Periodic review of logical and physical user access rights shall be conducted, and appropriate actions will be taken on the cases of non-conformities.

18.7 Logging and Monitoring activities

The purpose of logging and monitoring user activities is to detect network intrusions and compliance violations in the environment.

Policy Statement

- Logging all events, activities and transactions is a must in all government critical systems. Audit logs must include – user ids, date, time, terminal id, record of both successful and unsuccessful attempts, data, records and transactions, total access logs etc.
- The Government shall ensure that records of user access are uniquely identified and logged for audit and review purposes.

- Such audit logs must be available to only authorized users (to be authorized by CISO) in read-only format. Necessary reports must be easily available to those who are having monitoring responsibilities.
- System monitoring such as review of events, exceptions, accesses – is a must and appropriate reports must be available.
- Access to system files including audit log files, password files, and signature files must be restricted and these must be appropriately protected.

18.8 Administrator Password Management

Administrator accounts must be monitored to ensure that the privileged access in not being utilized in an inappropriate manner.

Policy Statement

- Administrator account details shall be stored securely and access to the same shall be restricted to the IT representative. Usage of generic ids shall be minimized and if used, these ids are to be mapped to designated IT administrators to ensure accountability.

18.9 Secure Log-on Procedures

Secure log on procedures must be followed to ensure that only the authorized users gain access to the organization's systems.

Policy Statement

- Employees of the government shall follow secure log on procedures while logging into their computing devices and applications.

18.10 Use of Privileged Utilities

There should be a restriction on use of privileged utilities to prevent unauthorized access.

Policy Statement

- The access to privileged utility programs shall be restricted only to the IT team as they perform the role of system administrators. Other employees shall not have access to such programs.

18.11 Application and Information Access Control

There should be a restriction on use of critical applications to prevent unauthorized access.

Policy Statement

- Access to government information and applications by government

employees shall be restricted in accordance with the defined access control policy defined by the government.

18.12 Session Time – Out

Sessions must be timed out when inactive for a certain time period to ensure that no unauthorized access takes place.

Policy Statement

- Inactive sessions on the government's employee computing devices and applications shall be configured for a lock out period.

18.13 Mobile Computing

Controls must be in place for handling mobile devices. Failure to do so might result in leakage of data from the mobile devices and might be used by unauthorized personnel.

Policy Statement

- Government employees are granted access to mobile computing devices and shall be periodically trained to protect against the risks of using mobile computing facilities.
- The government shall ensure that the devices are assigned to the appropriate personnel, and the details of the device allocation shall be tracked by the IT team.

18.14 Citizen Authentication

In the absence of appropriate controls for citizen authentication there is a risk of impersonators gaining access to critical citizen information.

Policy Statement

- Government shall implement authentication framework/mechanism to provide positive identify verification of government to citizens. Citizen identity information shall be kept secure. Government shall act as the identity provider for identification and authentication of citizens for access to partner systems using secure authentication technologies.

19. Antivirus Management

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, thumb drives, and CDs etc. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of the government is to provide a computing network that is virus free. The purpose of this policy is to provide instructions on measures that must be taken by government employees to help achieve effective virus detection and prevention.

19.1 Anti – Virus Updates

The anti-virus software must be updated regularly to ensure that all critical updates are available and the systems are protected against the latest threats.

Policy Statement

- All computers attached to the government network must have standard, latest version and supported anti-virus software installed. This software must be active, be scheduled to perform virus checks at regular intervals, and have its virus definition files kept up to date.
- Any activities with the intention to create and/or distribute malicious programs onto the Governments network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
- If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to UT Administration of DNH and Daman & Diu helpdesk immediately with a copy to the CISO. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
- No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.
- Any virus-infected computer will be removed from the network until it is verified as virus-free.

19.2 Scanning Government's Computing Devices

Regular scanning of all computing devices is essential to ensure that all systems are secure.

Policy Statement

- All Government computing devices shall be scanned for threats and viruses on periodic basis.

19.3 Rules for Virus Prevention

A guideline is essential to ensure that rules of virus prevention are established and available for reference if required.

Policy Statement

UT Administration of DNH & Daman and Diu shall enforce below guidelines on its employees and contractors to protect its critical assets from Virus attack.

- Always run the standard anti-virus software provided by the Government.
- Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
- Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.
- Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
- Files with the following filename extensions are blocked by the e-mail system: [.exe, .bat etc.]. Business files with banned extensions can be sent/received by compressing the same in a folder by use of a file compression utility.
- Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
- Avoid direct disk sharing with read/write access.
- If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
- The IT department/NIC will assist employees in installing anti-virus software according to standards on personally-owned computers that will be used for business purposes. The IT department will provide anti-virus software in these cases.
- The IT department/NIC will attempt to notify users of Government systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.
- External Parties should regularly update virus protection on their computers that are used for Government's purpose. This includes installing recommended security patches for the operating system and other applications that are in use.

20. Social Engineering – Protection against Online Fraud

Social engineering, also known as "pretexting," is used by many criminals, both online and off, to trick unsuspecting people into giving away their personal information and/or installing malicious software onto their computers, devices or networks.

20.1 Train employees to recognize social engineering

Social engineering leads to dangerous security lapses and is notoriously difficult to prevent. The UT Administration of DNH and Daman & Diu must ensure that its employees are trained to spot the most obvious red flags.

Policy Statement

The government shall train its employees to ensure the following:

- Users should not install malicious computer software such as fake antivirus.
- As technology evolves rapidly, the government shall ensure that all relevant personnel are getting proper training, education, updates and awareness of the cyber security activities as relevant with their job function.
- User responsibilities:
  - Users should not share critical organizational information on public sites or via email, and do not respond to email solicitations for personal/ financial information
  - Users should not send sensitive information over the Internet without checking the website's security and URL. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (Like: .com vs .net)
  - Change passwords in case suspected has been compromised.
- Government shall ensure adequate training/awareness facilities for internal audit team considering any new government services and technological changes.

20.2 Protection against Phishing

Phishing is the technique used by online criminals to trick people into thinking they are dealing with a trusted website or other entity. An organization should have controls in place to recognize such threats and take appropriate measures.

Policy Statement

- Governments shall make a clear statement in its communications reinforcing that it will never ask for personal information via email so that if someone targets citizens, they may realize the request is a scam.
- Employee awareness is a best defense against users being tricked into handing over their usernames and passwords to cyber criminals. Government shall conduct user/employee/citizens awareness session and update them –

  - To NEVER respond to incoming messages requesting private information and also avoid being led to a fake site.
  - DO NOT open emails in the spam folder or emails whose recipients you do not know.
  - DO NOT open attachments in emails of unknown origin.
  - UPDATE the employees needing to access a website link sent from a questionable source should open an Internet browser window and manually type in the site’s web address to make sure the emailed link is not maliciously redirecting to a dangerous site.

20.3 Avoid Installation of Fake Antivirus

Fake antivirus and other rogue online security scams have been behind some of the most successful online frauds in recent times. Government shall train its employees to recognize a legitimate warning message and to properly notify its IT team if something bad or questionable has happened.

Policy Statement

- Administrative access for the regular users shall be restricted to authorized individuals only. This will minimize the risk of such users installing malicious software and educate the users that adding unauthorized software to work computers is against the government's Information Security policy.
- Government shall develop a procedure explaining the procedure that needs to be followed if an employee's computer becomes infected by a virus.

21. Protection Against Malware

Government's Information systems can experience a compromise through the introduction of malicious software, or malware, that tracks a user's keyboard strokes, also known as key logging. Once installed on the system, the malware can record keystrokes made on a computer, allowing hackers to see passwords, credit card numbers and other confidential data. Other malwares include virus, worms, Trojans, spyware, adware and Bots.

Policy Statement

- The government shall keep the anti-malware software up to date and also regularly patch its computer systems that will make it more difficult for any type of malware to infiltrate its network.

22. Systematic approach for protection against malicious Software.

Effective protection against viruses, Trojans and other malicious software requires a systematic approach to its defenses. Antivirus software is a must, but should not be government only line of defense. Governments should deploy a combination of various defense techniques to keep its environment safe.

Policy Statement

- Government shall build a robust defense against the installation, spread, and execution of malicious code at multiple points in the enterprise.
- Government shall implement Anti-malware, Antivirus protection including behavioural detection systems for all categories of devices – (Endpoints such

as PCs/laptops/ mobile devices etc.), servers (operating systems, databases, applications, etc.), Web/Internet gateways, email-gateways, Wireless networks, SMS servers etc. including tools and processes for centralized management and monitoring

- Government shall consider implementing whitelisting of internet websites/systems.
- Government shall consider implementing secure web gateways with capability to deep scan network packets including secure (HTTPS, etc.) traffic passing through the web/internet gateway
- Government shall consider combining the use of web filtering, antivirus signature protection, proactive malware protection, firewalls, strong security policies and employee training to significantly lower the risk of infection.
- Government shall keep protection software up to date along with the operating system and applications to increase the safety of the systems.

23. Third Party Security

Third party security plays an important role in the protection of end user's privacy. Actively monitor such third parties for compliance of contractually defined process and NDA (Nondisclosure agreement). Employees of third parties / vendors providing services from the government premises shall adhere to the UT Administration of DNH and Daman & Diu Cyber Security Policy.

Policy Statement:

- The government shall fully understand risks associated with ICT outsourcing. Before appointing a service provider, due diligence shall be carried out to determine its viability, capability, reliability, track record and financial position.
- The Government shall ensure that contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out fully in written agreements
- Outsourcing activities shall be evaluated based on the following practices:
    - Objective behind Outsourcing
    - Economic viability
    - Risks and security concerns.
- Outsourcing shall not result in any weakening or degradation of the government's internal controls. The Government shall require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive or confidential information, such as citizen data, object programs and source codes.
- The Government shall require the service provider to implement security policies, procedures and controls that are at least as stringent as it would expect for its own operations.
- The Government shall monitor and review the security policies, procedures and controls of the service provider on a regular basis, including periodic expert reports on security adequacy and compliance in respect of the

operations and services provided by the service provider.

- Government shall require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures
- Government shall develop a contingency plan for critical outsourced technology services to protect them from unavailability of services due to unexpected problems of the technology service provider. This may include termination plan and identification of additional or alternate technology service providers for such support and services
- Government shall maintain an updated list of all third-party services received preserving up-to-date information of each service rendered, service provider name, service type, SLA expiry date, service receiving manager, service reporting, emergency contact person at service provider, last SLA review date, etc.
- The Government shall provide official authorization/assurance from the group ensuring the data availability and continuation of services for the circumstances e.g. diplomacy changes, natural disaster, relationship breakdown, discontinuity of services, or others.
- The Disaster Recovery Site shall be multi-layered in terms of physical location and redundancy in connectivity.
- There shall have Service Level Agreements between the Government and vendors.
- The Annual Maintenance Contract (AMC) with the vendor shall be active and currently in-force.
- Dashboard with significant details for SLAs and AMCs shall be prepared and kept updated.
- Government shall ensure that the equipment does not contain sensitive live data when hardware is taken by the service provider for servicing/ repairing.

  The requirements and conditions covered in the agreements would usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.
- Service contracts with all service providers including third-party vendors shall include:
  a) Pricing
  b) Measurable service/deliverables
  c) Timing/schedules
  d) Confidentiality clause
  e) Contact person names (on daily operations and relationship levels)
  f) Roles and responsibilities of contracting parties including an escalation matrix
  g) Renewal period
  h) Modification clause
  i) Frequency of service reporting

j) Termination clause
k) Penalty clause
l) Warranties, including service suppliers' employee liabilities, 3rd party liabilities and the related remedies
m) Geographical locations covered
n) Ownership of hardware and software
o) Documentation (e.g. logs of changes, records of reviewing event logs)
p) Right to have information system audit conducted (internal or external).

24. Cloud Security

Cloud Computing is a new computing model originating from grid computing, distributed computing, parallel computing, virtualization technology, utility computing and other computer technologies. It exhibits many advantages such as large-scale computation and data storage, virtualization, high expandability, high reliability and low-price service. However, trust and security in Cloud Computing are more complex than in a traditional IT system. In order to have a secure Cloud Computing deployment, it is necessary to consider the following areas: the Cloud Computing architecture, governance, portability and interoperability, traditional security, government continuity and disaster recovery, data centre operations, incident response, notification and remediation, application security, encryption and key management, identity and access management. The government shall choose a cloud service provider if they demonstrate compliance with essential security requirements. But, first priority is to preferred government cloud then any private organization cloud in case if it's required then proper steps followed by signing NDA and with senior management level authorization.

Policy Statement

- Each provider's cloud computing security policy document shall be approved by senior management, and published and communicated to all employees and relevant external parties either as part of the organization's information security policy or as a separate policy. The policy should set the goals and objectives governing the cloud computing service.
- The government shall request and assess the detailed information on how the cloud service provider ensures and applies agile and rapid yet comprehensive risk management prior to contracting the provider.
- The government shall ask and validate the provider's risk control checking methodology or ensure that information security policy conforms to international best practices.
- Cloud service provider shall provide the government with its complete vendor list that will have access to government's data; at any point throughout the duration of the agreement. The provider shall also update the agency with any change in the vendor list.
- The government shall not grant the cloud service provider permissions to

directly use/access the organization authentication environment such as the organization's main directory.

- The government shall ensure that the cloud service provider's authentication process, access control, accountability and logging (Format, retention and Access) meet the government's regulatory and legal requirements.
- The Government shall train their IT staff on accessing and using the Cloud Service provider log services
- The government shall ensure logging is enabled for all security events (covering sessions and transaction information) for a period as prescribed by statutory or regulatory authorities.
- The government shall ensure that the cloud service provider adopts and is in compliance with change management and incident response procedures.
- The government shall review the service provider's DR plan and ensure it matches the government requirements
- The government shall ensure that SLAs reflect he applications and data high availability requirements (as per the government's GIA or government requirements) in the event of planned or unplanned disruptions or outages, with government continuity and disaster recovery planning and backup and redundancy mechanisms reviewed by the government
- SLAs should define financial remedies in the event of a service disruption.
- The government shall ensure that data is encrypted at storage and in transit and in full compliance (at any given point in time) with the government approved cryptographic algorithms and protocols.
- The government shall train its responsible staff on vendor management and cloud technologies.
- The government shall define and document the different roles and responsibilities for the staff responsible for managing the cloud service.
- The service provider shall sign an NDA with the government before provisioning any service.

  The government shall ensure that it retains the "Exclusive" right to data ownership throughout the duration of the agreement. The ownership includes all copies of data available with the service provider including backup media copies if any. Government shall require that service providers are not permitted to use government's data for advertising or any other non-authorized secondary purpose.
- The government shall "specify" in the contract the country(s) where it is acceptable for the data to be stored.
- The government shall contractually ensure that they are "immediately" notified of any confirmed breach without any undue delay.
- The government shall contractually state that the service provider will completely delete/eliminate any trace of Data/information at the end of the Agreement as agreed in the agreement.
- The government shall contractually state and ensure that the service provider will comply with the data and media destruction and sanitization controls.
- The government shall ensure that the service provider supports the return of

data to the government. There should be no Vendor-lock in by the service provider.

- The government shall develop a roadmap to adopting and integrating cloud computing because of the complexity of the cloud environment that introduces a number of unknown variables for which government and public services will need to build new approaches to assess and manage the associated risks.
- The government shall always keep and maintain the capability of backtracking from the adoption of a cloud solution.

25. Disaster Recovery

25.1 Data Backup and Recovery Plan

The purpose of having a data back-up is defining a strategy for identification of critical information, planning for back-up and implementing the same in an effective manner. Data loss situation can arise due to power failure, system crash, viruses, zero-day attacks, malwares, APTs, intentional or unintentional data handling etc., therefore guidelines under this control shall be in place to reduce the impact of data loss.

Business Continuity and Disaster Recovery Management is required for planning of business resiliency for critical incidents, operational risks take into account for wide area disasters, Data Centre disasters and the recovery plan. The primary objective of Government Continuity Plan (GCP) is to enable a Government to survive in a disaster and to re-establish normal government operations. In order to survive with minimum financial and reputational loss, Government shall assure that critical operations can resume normal processing within a reasonable time frame. The contingency plan shall cover the government service resumption planning and disaster recovery planning. Contingency plan shall also address the backup, recovery and restore process.

Policy Statement

- The government has established a policy for information backup encompassing cyber resilience measures. The Government shall develop a data backup and recovery policy. Each business application must have a planned, scheduled and documented backup strategy, involving the making of both on- and off- line backups and the transfer of backups to secure offsite storage.
- Details of the planned backup schedule for each government application must be created in line with the classification of the application and the information it supports and must specify the type of back-up required (full, partial, incremental, differential, real-time monitoring) at each point in the back-up schedule.

- The frequency of backups taken for information must be determined in line with the classification of the information and the requirements of the government continuity plans for each application. The details of the planned backup schedule for each business application must include the retention period for backed-up or archived information and the retention period must be consistent with local legal and regulatory requirements.
- All media contained backed-up information must be labelled with the information content, backup cycle, backup serial identifier, backup date and classification of the information content. The backup inventory and log sheet shall be maintained, checked and signed by the supervisor. The Government shall encrypt backup data in tapes or disks, containing sensitive or confidential information, before transported offsite for storage.
- At least one copy of backup shall be kept on-site for the time critical delivery. The process of restoring information from both on- and off-site backup storage must be documented. The Government shall carry out periodic testing and validation of the recovery capability of backup media and assess whether it is adequate and sufficiently effective to support the government's recovery process.

25.2 Disaster Recovery

A disaster recovery site (DR Site) is a site where data is synchronized from Production site to DR Site. In the event of disaster, DR Site will host the essential/bare minimum services to run the critical operation of the organization. DR site plays an important role to run critical government service process during adverse situations.

Policy Statement

The government has established a policy for information government service continuity management encompassing cyber resilience measures of best industry practices.

- Government must have an approved Disaster Recovery Plan. In formulating and constructing a rapid recovery plan, the Government shall include a scenario analysis to identify and address various types of contingency scenarios. The Government shall consider scenarios such as major system outages which may be caused by system faults, hardware malfunction, operating errors or security incidents as well as a total incapacitation of the primary DC.
- The Government shall establish a Disaster Recovery Site (DRS) which is geographically separated from the primary site (minimum of 10 kilometers radial distance but choice of different seismic zone will be preferred) to enable the restoration of critical systems and resumption of government operations when a disruption occurs at the primary site. If Disaster Recovery Site (DRS) is not in different seismic zone, Government may establish a third site

in different seismic zone which will be treated as Disaster Recovery Site (DRS)/Far DC. In such case the DRS in near location will be treated as Near DC and shall be configured accordingly.

- DRS and/or Near DC shall be equipped with compatible hardware and telecommunication equipment to support the critical services of the government operation in the event of a disaster. Physical and environmental security of the DRS and/or Near DC shall be maintained. The Government shall define system recovery and service resumption priorities and establish specific recovery objectives including recovery time objective (RTO) and recovery point objective (RPO) for ICT systems and applications. RTO is the duration of time, from the point of disruption, within which a system shall be restored. RPO refers to the acceptable amount of data loss for an ICT system while a disaster occurs.
- The Government shall consider inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests. The Government may explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance the government's recovery capability. Information security shall be maintained properly throughout the recovery process. An up-to-date and tested copy of the DR plan shall be securely held off-site. One copy shall be stored in the office for ready reference.
- The Government shall test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures. Such testing shall also include testing of crisis communication to citizens and other internal and external stakeholders.

The Government shall involve its government users in the design and execution of comprehensive test cases to verify that recovered systems function properly. DR test documentation shall include at a minimum of Scope, Plan and Test Result. Test report shall be communicated to management and other stakeholders and preserved for future necessity.

25.3 Contingency Planning

Contingency plan deals with the alternate methods of operation in case of emergency. This planning also deals with the restoration of all affected services within defined time duration. The entire aim of the contingency planning is to reduce the impact of the disaster to the minimum as it is challenging to completely eliminate the loss caused due to these disruptions.

Policy Statement

The government shall incorporate and materialize contingency plan in risk assessment and treatment methodology. UT Administration of DNH and Daman & Diu must have an approved government Continuity Plan addressing the recovery from disaster to continue its operation. Approved GCP shall be circulated to all

relevant stakeholders. The recipients would receive a copy of amended plan whenever any amendment or alteration takes place. Documents related to GCP must be kept in a secured off-site location. One copy shall be stored in the office for ready reference. The GCP shall be coordinated with and supported by the Government Impact Analysis (GIA) and the Disaster Recovery Plan (DRP) considering system requirements, processes and interdependencies.

GCP shall address the followings:

a) Action plan to restore government operations within the specified time frame for:
   i. Office hour disaster
   ii. Outside office hour disaster.
b) Emergency contacts, addresses and phone numbers of employees, vendors and agencies.
c) Grab list of items such as backup tapes, laptops, flash drives, etc.
d) Disaster recovery site map

GCP must be tested and reviewed at least once a year to ensure the effectiveness.

26. Mobile Device Security

26.1 Cyber Plan Action Items

All mobile devices that connect to the government network must be equipped with security software and password protection; and providing general security training to make employees aware of the importance of security practices for mobile devices.

Policy Statement

- Users must Use security software on all mobile devices.
- With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.
- Users must make sure all software is up to date.
- Users must not load pirated software or illegal content onto their devices.
- Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If a user is unsure if an application is from an approved source contact IT department/NIC.
- Data must be encrypted on mobile devices.
- The users with password protected access to mobile devices shall be allowed. In addition to encryption and security updates, it is important to use strong passwords to protect data stored on mobile devices.
- The government shall urge users to be aware of their surroundings.
- Users shall only load data essential to their role onto their mobile device(s).
- Devices shall not be connected to a PC which does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.

- The government shall employ these strategies for email, texting and social networking
  - Avoid opening unexpected text messages from unknown
  - Don't be lured in by spammers and phishers
  - Click with caution
- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that government data is only sent through the government email system. If a user suspects that government data has been sent from a personal email account, either in body text or as an attachment, they must notify Helpdesk immediately.
- Users must not use government workstations to backup or synchronize device content such as media files unless such content is required for legitimate government purposes.
- The government shall set reporting procedures for lost or stolen equipment.
- If a user suspects that unauthorized access to government data has taken place via a mobile device then user must report the incident in alignment with government's incident handling process.
- The government end user must ensure all devices are wiped clean prior to disposal.

***To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.**

27. Internet banking or any transaction Security

Internet banking or any transaction security is of utmost importance as it is one of the most important methods of financial transactions. In the absence of an appropriate internet security controls, there is a risk of online fraud, inappropriate use of citizen information and damage to the government name.

Policy Statement

- Government shall ensure suitable security measures for the web applications and reasonable mitigation measures against various web security risks.
- Government shall ensure that web applications do not store sensitive information in HTML hidden fields, cookies, or any other client-side storage leading to compromise in the integrity of the data. Critical web applications of Government shall enforce at least SSL v3 or extended Validation – SSL / TLS 2.0/3.0 128/256-bit encryption level for all online activity.
- Government shall follow a defense in depth strategy by applying robust security measures across various technology layers.
- Governments shall implement appropriate measures to minimize exposure

to a middleman attack which is more commonly known as a man-in-the-middle attack (MITM), man-in-the browser (MITB) attack or man-in-the application attack.

28. Data Leakage Prevention

Data security is paramount for all services especially governments. Citizen's personally identifiable information, financial details and such critical information is often impossible to replace if lost and highly dangerous in the hands of criminals. Data loss due to natural events such as floods, fire causes huge government impact, but losing such sensitive data to cyber criminals will have profound effect on government bottom line and even its very continued existence. Consequences of data loss or leakage could be:

- Loss of productivity or downtime
- Loss of public trust on Government
- Loss of certifications, licenses, ratings, etc.
- Civil lawsuits resulting in monetary judgments and/or injunctions

Policy Statement

Data Leakage Prevention strategy plays a crucial role in protection of critical data. The following are the activities that could ensure effective protection of Data:

- The Government shall classify the data to accurately identify the sensitivity level of data and the impact of loss or disclosure of each data set. Sensitive data falls under these categories:
    - Restricted
    - Confidential
    - Internals
- Government shall develop safeguard mechanism to protect its sensitive data in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.
- The Government shall setup safeguards against the unintentional and/or unauthorized moving or copying of sensitive data to unprotected devices via email, through permitted BYOD devices, removable media, etc.
- The Government shall document and track DLP incidents.
- Government shall perform control remediation or implementation of new safeguards as and when DLP incident has occurred
- The Government shall train its employees against social engineering, phishing and Malwares
- The Government shall ensure that vendors adhere to the Government's Data loss/leakage prevention strategy.

29. Removable Media Security and BYOD (Bring Your Own Device)

The Government, in future, may decide to implement a policy to enable the employees to bring in and connect their own devices (such as smartphones, tablets and laptops) to official network for official use which includes sharing of official information only. Removable USB devices, especially USB storage like portable Hard Disk, pen drive, CD, etc., shall be used strictly for official purpose and use of the same has to be authorized by head of department/office. The user should also ensure that external devices are free from any virus/malware. The user as well as data owner would be responsible for leakage of any sensitive/ critical data/ spread of virus or malware etc.

The BYOD policy statements mentioned below shall be applicable only once the Government decides to roll it out to its employees and will be applicable on the devices specifically permitted by the Government for Government's service purposes.

Policy Statement

- All the devices which are connected to official network shall be accounted for, classified and handled depending on their sensitivity and importance.
- Government shall implement a BYOD acceptable use policy, agreed and signed by each person using a BYOD device.
- Government personnel shall have written authorization (usually managerial approval) before a connection is enabled. Written authorization shall include the nature and extent of government access approved, considering:
  - time, day of the week
  - location
  - local or roaming access
- Standard Operating Procedures for the government's BYOD network shall be established.
- Provision shall be made for contractors and other authorized non-employees. Ownership of data on BYOD devices shall be clearly articulated and agreed
- Individuals shall be responsible for the installation and maintenance of any mandated BYOD-based firewalls and anti-malware software and for implementing operating system updates and patches on their device
- The BYOD network segment shall be segregated from other elements of government's network
- Government shall architecturally separate guest and public facing networks from BYOD networks
- Access to internal resources and servers shall be carefully managed and confined to only those services for which there is a defined and properly authorized business requirement
- Bluetooth on BYOD devices shall be disabled while within designated secure areas on government premises
- Government shall check each BYOD device for malware and sanitize the device appropriately before installing software or operating environments
- BYOD shall have a Mobile Device Management (MDM) solution implemented

with a minimum of the following enabled:

- The MDM is enabled to "wipe" devices of any government data if lost or stolen
- If the MDM cannot discriminate between government and personal data, all data, including personal data, is deleted if the device is lost or stolen;
- The MDM is capable of remotely applying government security configurations for BYOD devices;
- Mobile device security configurations are validated (health check) by the MDM before a device is permitted to connect to the government's systems;
- "Jail-broken", "rooted" or settings violations MUST be detected and isolated;
- "Jail-broken" devices are NOT permitted to access government resources;
- Access to government resources is limited until the device and/or user is fully compliant with policy and SOPs;
- Auditing and logging are enabled; and
- Changes of Subscriber Identity Module (SIM) card is monitored to allow remote blocking and wiping in the event of theft or compromise.

- Government shall block the use of unapproved cloud applications for processing any data
- BYOD devices shall not be permitted direct connection to internal hosts, including all other devices on the local network
- BYOD devices connecting to guest and public facing networks shall not be permitted access to the corporate network other than through a VPN over the Internet.
- BYOD devices and systems shall use Multifactor (at least two-factor) authentication to connect to systems and prior to being permitted access to confidential data.
- Any government data exchanged with the mobile device shall be encrypted in transit
- Any government data stored on the device should be encrypted (including keys, certificates and other essential session establishment data).
- The use of virtual containers, sandboxes, wraps or similar mechanisms on the mobile device shall be established for each authorized session for any organizational data.
- Any sensitive government data shall be removed/securely deleted, or encrypted at the end of a session
- Connections to the government network shall be time limited
- Communications between the mobile device and the government network shall be established through a Virtual Private Network (VPN)
- Government shall disable the ability for a BYOD device to establish simultaneous connections (e.g. wireless and cellular) when connected to the network.
- The use of passwords or PINs to unlock the BYOD device shall be enforced in addition to authentication mechanisms government access
- Device passwords shall be distinct from any government access and authentication passwords.
- Government shall compile a list of approved BYOD devices and operating systems for the guidance of staff

- Government shall consider the use of bandwidth limits as a means of controlling data downloads and uploads

30. Cyber Audits

30.1 Cyber Security Audit

Cyber security audits are essential to address any underlying threats and to ascertain compliance of the organization's policy.

Policy Statement

Cyber security audit shall be a part of IT audit and the report for the same shall be presented to the management by CISO followed by the closure tracker of gaps identified in the audit. The government shall conduct cyber security audit on a bi-annual basis. The scope of cyber security audit shall include:

i. Determining effectiveness of planning and oversight of cyber activities
ii. Evaluating adequacy of operating processes and internal controls
iii. Determining adequacy of enterprise-wide compliance efforts, related to cyber policy and procedures.
iv. Identifying areas with deficient internal controls, recommend corrective action to address deficiencies and follow-up, to ensure that the management effectively implements the required actions.

30.1.1 Planning Cyber Security Audit

Policy Statement

- The government shall use Risk Based Audit Approach while planning a cyber- security audit. Government shall develop a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators.

30.1.2 Execution of Cyber Security Audit

Policy Statement

- The government in consultation with auditor would describe steps for executing the audit, covering activities such as understanding the government process and cyber environment, refining the scope and identifying internal controls, testing for control design and control objectives, audit evidence, documentation of work papers and conclusions of tests performed.

30.1.3 Reporting and Follow-up

Policy Statement

- The cyber security audit findings shall be reported to the management with the closure status/ roadmap provided by CISO. Auditors would prepare an audit summary providing overview of the entire audit processing from planning to audit findings, discuss the findings with respective personnel and obtain responses.

30.2 Compliance with Security Recommendation

Based on the findings of the audit all security recommendations must be implemented within an appropriate timeframe to ensure that all risks are addressed and appropriate measures are taken.

Policy Statement

- Practices in accordance to the Cyber Security Policy along with compliance of security recommendations from cyber security audit reports shall be followed by the government employees.

30.3 Learning and Evolving

A cyber resilience framework needs to ensure continuous cyber resilience amid a changing threat environment. To be effective in keeping pace with the rapid evolution of cyber threats, government shall implement an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks and allows the government to identify, assess and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. A government shall aim to instil a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

Policy Statement

- Government shall systematically identify and distil key lessons from cyber events that have occurred within and outside the organization in order to advance its resilience capabilities. Useful learning points can often be gleaned from successful cyber intrusions and near misses in terms of the methods used and vulnerabilities exploited by cyber attackers.
- Government shall actively monitor technological developments and keep abreast of new cyber risk management processes that can effectively counter existing and newly developed forms of cyber-attack. Government shall consider acquiring such technology and know-how to maintain its cyber resilience.
- Government's cyber risk management practices shall go beyond reactive controls and include proactive protection against future cyber events.

Predictive capabilities and anticipation of future cyber events are based on analyzing activity that deviates from the baseline. Government shall work towards achieving predictive capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity.

- Metrics and maturity models allow to assess its cyber resilience maturity against a set of predefined criteria, typically its operational reliability objectives. This benchmarking requires the government to analyze and correlate findings from audits, management reviews, incidents, near misses, tests and exercises as well as external and internal intelligence gathered. The use of metrics can help to identify gaps in its cyber resilience framework for remediation, and allow the government to systematically evolve and achieve more mature states of cyber resilience.

31. Awareness

Policy Awareness shall be attained by making the policy available to the employees over the intranet. Training sessions, covering the various aspects of the Cyber Security policy, shall be carried out for the new joiners and refresher sessions for the existing employees on a periodic basis.

3.1 User/Employee Awareness

The employees in an organization are its first line of defence. Hence it is essential that all users/ employees are made aware of the policy.

Policy Statement

- Government shall define and communicate to users/employees, vendors & partners security policy covering secure and acceptable use of government network/assets including citizen information/data, educating them about cybersecurity risks and protection measures at their level
- Government shall encourage users and employees to report suspicious behavior incidents to the incident management team.
- Government shall conduct targeted awareness/training for key personnel (at executive, operations, security related administration/operation and management roles, etc.)
- Government shall evaluate the awareness level periodically.
- Government shall establish a mechanism for adaptive capacity building for effective Cybersecurity
- Management. Making cyber security awareness programs mandatory for new recruits and web-based quiz & training for lower, middle & upper management every year.
- Board members shall be sensitized on various technological developments and cyber security related developments periodically.
- Board members shall be provided with training programmes on IT Risk /

Cybersecurity Risk and evolving best practices in this regard so as to cover all the Board members at least once a year.

31.2 Citizen Awareness

With the advent of electronic government service, citizen experience of government service is therefore no longer fully under control of a government. In the age of self-service government model, a citizen also has to be equipped to do safe use of government application through self-help. It is often said that the best defence against frauds is awareness of citizens. With fraudsters constantly creating more diverse and complex fraudulent ruses using advanced technology and social engineering techniques to access their victims' data, accelerating awareness among citizens becomes imperative. It is also important to educate other stakeholders, including government employees, who can then act as resource persons for citizen queries, law enforcement personnel for more understanding response to citizen complaints and media for dissemination of accurate and timely information.

Policy Statement

To implement a successful awareness program, UT Administration of DNH and Daman & Diu shall ensure the following:

- The needs of the target audience shall be identified and priorities established.
- The work plan shall clearly mention the main activities with the required resources, timelines and milestones.
- The Government shall create and publish proper contents.
- The common objectives of the awareness program will be to:
- Provide general and specific information about fraud risk trends, types or controls to people who need to know.
    - Help citizens to identify areas vulnerable to fraud attempts and make them aware of their responsibilities in relation to fraud prevention.
    - Motivate individuals to adopt recommended guidelines or practices.
    - Create a stronger culture of security with better understanding and commitment.
    - Help minimize the number and extent of incidents, thus reducing costs directly (fraud losses) and indirectly (reduced need to investigate).
- The Government shall deliver the right message content to the right audience using the most effective communication channels.
- Awareness building collaterals can be created in the form of:
    - Leaflets and brochures
    - Short Messaging Service (SMS) texts
    - Educational material for cyber security to students.
    - Receipts dispensed at any service given to citizens.
    - Screensavers
    - Electronic newsletters

    - Social media platform uses with animated case studies and videos
- Recorded messages played during waiting period of IVR calls
- Since the target groups obtain information from a variety of sources, more than one communication channel could be used to engage them successfully.
    - Advertising campaigns though print and TV media
    - Emails and SMS texts
    - Common website developed with content from all stakeholders
    - Groups, games and profiles on social media
    - Advertisements on online shopping sites
    - Bill boards
    - Online training modules and demos hosted on website
    - Posters in prominent locations such as schools/colleges, petrol pumps, popular restaurants, shopping malls, etc.
    - Interactive guidance in the form of helplines
    - Talk shows on television/radio
- Continuous improvement cannot occur without knowing how the existing program is working. A well-calibrated feedback strategy must be designed and implemented.

32. Child Online Privacy Protection Act (COPPA).

COPPA applies to children under the age of 13 who use the internet. The legislation aims to protect children's personal information when they access online services, games, apps, or websites. COPPA was created due to the recognition that children's personal information is more sensitive than adults', and they may have difficulty understanding the potential consequences of providing personal data online.
COPPA requires websites, apps, games, and online services that collect personal information from children to provide clear and understandable notices to parents and get verifiable parental consent before collecting, using, or disclosing children's personal information. The following are some examples of the type of information that COPPA protects:

- Full name
- Home address
- Email address
- Phone number
- Aadhaar number
- Information collected online, such as IP address, geolocation data, and behavioral data

What Privacy Rights Do Children Have Under COPPA?

Children have several privacy rights under COPPA, including:

1. The right to know what personal information is being collected from them
2. The right to opt out of the collection of personal information

3. The right to have their personal information deleted upon request
4. The right to refuse to disclose personal information to a website or app

32.1 How Are Children's Rights Upheld Under COPPA?

Policy Statement

Websites and apps must uphold these rights by providing notice to parents about the types of personal information collected from their children, obtaining verifiable parental consent before collecting personal information, and giving parents the option to review and delete their children's personal information at any time.

32.2 The Roles Parents and Guardians Play With COPPA.

Parents and guardians play a significant role in protecting their children's online privacy.

Policy Statement

- COPPA requires that companies obtain verifiable parental consent before collecting any personal information from children.
- This means that companies must take appropriate steps, such as sending a confirmation email, to ensure that the person providing consent is the child's parent or legal guardian.
- In addition, COPPA mandates that companies provide parents with the right to review their children's personal information and ask for it to be deleted.
- Parents should talk to their children about the dangers of sharing personal information online and monitor their kids' online activity regularly. Educating children on the importance of online privacy is critical in today's digital age.

32.3 The Roles Website Owners and Operators Play With COPPA

COPPA has significant implications for websites, apps, and online services that collect personal information from children.

Policy Statement

- Website owners and operators must ensure they comply with COPPA's requirements to avoid facing legal action from the UT Administration of DNH & DD. Failure to comply with COPPA can result in monetary and legal penalties.
- To comply with COPPA, website owners and operators must provide clear and easily

understandable privacy policies to parents. These policies must inform parents of the personal information collected from children, how it's used, and whether it's shared with third parties.

- Website owners and operators must also obtain verifiable parental consent before collecting personal information from children. They can do this by sending a confirmation email or asking parents to provide personal information that can be checked against public records.

32.4 COPPA, Social Media, and User-generated Content

COPPA has had a significant impact on technology companies, particularly social media and messaging apps.

Policy Statement

- COPPA applies to social media sites and user-generated content that is directed at children under the age of 13.
- It requires social media sites to obtain verifiable parental consent before collecting personal information from children and to provide notice to parents about the types of personal information collected.

32.5 What Are the Requirements for Social Media Sites Under COPPA?

Policy Statement

- Social media sites must comply with the same requirements as other websites and apps under COPPA, including providing notice to parents about the types of personal information collected, obtaining verifiable parental consent before collecting personal information, and giving parents the option to review and delete their children's personal information at any time.
- In addition, social media sites must provide a clear and conspicuous link to their privacy policy from their homepage and within any online service directed at children.

32.6 COPPA and Schools

Schools and educational institutions are also subject to COPPA's requirements. Schools must comply with COPPA when using online services, apps, and websites that collect personal information from children.

Policy Statement

- Schools must obtain verifiable parental consent before allowing children to access online services, and they must ensure that they are using COPPA-compliant services.
- COPPA has had a significant impact on online educational services, as many schools have had to adapt their online learning platforms to comply with COPPA's requirements.

- Online education service providers must obtain verifiable parental consent before collecting personal information from children and must ensure that their services have appropriate security measures to protect children's data.

When Is Parental Consent Not Required for COPPA?

Parental consent is not required under the following circumstances:

1. When a website or app collects personal information for the sole purpose of responding to a one-time request from a child
2. When a website or app collects personal information for internal use to improve the website or app, so long as the information is not disclosed to third parties
3. When a website or app collects personal information in connection with certain educational activities, such as online tutorials or contest.

33. Exceptions

Any exceptions to this policy must be duly approved by the Administrator/Secretary of the government.

34. Non-Compliance

Any non-compliance shall be subject to disciplinary action, up to and including termination of employment, contractual agreement/ obligation.

35. Policy Review

The Policy shall be reviewed by Department of IT at least on annual basis or as and when required, to ensure the policy is updated to take account of the changing circumstances, applicable laws and legislations, technology and security risks. Any revision to the policy has to be approved by the Board prior to implementation.

( ) **( )**

Secretary - IT **Director - IT**

Cyber Crisis Management Plan (CCMP) Version 1.0

1. Introduction.

Cyber Security is essentially a sub-set of Information Security. Deviating from the traditional Information Security policies, which need to be a regular hygiene among IT and Government teams, Cyber Security focuses on external attacks through various channels and control such attacks, along with maintaining strict controls on internal technology and processes which, if compromised, may lead to Cyber-attacks.
However, inspite of implementing various controls, nobody can guarantee as AI/ML increased the scope of attack and no guarantee that Cyber-attacks will not take place in the government. Therefore, with the increase in Cyber security breaches and attacks, it is important for the government to maintain a plan of action to respond to a Cyber security breach and a crisis situation.

In order to ensure a consistent and a practical approach in responding to Cyber security crisis, this document has been developed for adoption and use at UT Administration of DNH and Daman & Diu.

2. Authority

Oversight of the security of Government information technology resources and information is entrusted to CISO of the Government.

Cyber security Policy ver. 1.0 gives the CISO the authority to respond to threats to Government's networks, systems, and services. Government's **cyber security policy** states that evaluating and reporting cyber security incidents are important to ensure that information security events and weaknesses associated with information systems are communicated in a manner that will allow timely corrective action to be taken.

3. Purpose and Scope

This document seeks to assist Government personnel in mitigating the risks from cyber security incidents by providing a practical guide for responding to incidents effectively and efficiently. This document includes guidelines on establishing an effective cyber security incident response program, but the primary focus of the document is to provide assistance with detecting, analyzing, prioritizing and handling incidents.

This document is not intended to replace Continuity or Disaster Recovery Planning. It is not intended to be used as a detailed list to accomplish every task associated with cyber security incident handling and response. Rather, the document is intended to provide a framework and process by which consistent approach can be developed and resource allocations can be made for a given scenario to facilitate the detection, identification, containment, eradication, and recovery from specific cyber security incidents.

This document addresses only incidents that are IT security related, not those caused by natural disasters, power failures, etc.

This document applies to UT Administration of DNH and Daman & Diu owned computers and technology devices connected to the Government technology network at all locations.

This document is intended to provide guidance to address cyber security incidents that have impact on Government operational, financial, or reputational standing and/or the ability to comply with regulatory or legal requirements.

The field of cyber security is technology intensive and new vulnerabilities emerge with progress in AI/ML technology giving rise to new types of incidents. As such, the plan of response to cyber security incidents needs to be updated on regular basis, preferably once in a year.

4. Audience

This document has been created for UT Administration of DNH and Daman & Diu cyber incident response team (CIRT), Senior official, system and network administrators, security staff, technical support staff, Programmers, Chief information security officer (CISO) and others responsible for preparing for or responding to cyber security incidents at the Government.

5. Cyber Incident Response Capabilities

A cyber security incident can be defined as an occurrence that:

a) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality or availability of an information system or the information that system controls, processes, stores or transmits; or
b) Constitutes a violation or imminent threat of violation of law, security policies, security procedures or acceptable use policies.

An incident could be either intentional or accidental in nature.

Examples of cyber security incidents (hereafter may be referred to as “cyber incident” or “incident”) may include, but are not limited to:

- An incident in which an attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- An incident in which users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers, networks and established connections with an external host.
- An incident where an attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- An incident where a user provides or exposes sensitive information to others through peer-to-peer file sharing services.

Incidents similar to those noted above may be inflicted successfully at Government Network and may cause financial and reputational harm, disrupt daily operations and create compliance issues with standard requirements and regulatory laws. Establishing cyber incident response capabilities at the Government will ensure systematic (i.e., following a consistent cyber incident handling methodology) and coordinated actions required to be taken.

Incident response capabilities also build institutional resilience. Information gained and lessons learned during incident handling can help better to prepare for dealing with such future incidents.

6. Cyber Incident Response Team (CIRT)

In order to strengthen the cyber incident response capabilities a Cyber Incident Response Team (CIRT) will be constituted to coordinate the response activities. The Cyber Incident Response Team is composed of various members like CISO, Head of IT along with CIRT core IT team members that make up the CIRT.

6.1 Mission of CIRT

The Cyber Incident Response Team's (CIRT) mission is to:

- Limit the impact of cyber incidents in a way that safeguards the well-being of the Government's users (employees, citizens and vendors).
- Protect the information technology infrastructure of the Government.
- Protect sensitive Government data from disclosure, modification and exfiltration.
- Collect the information necessary to pursue investigation(s) at the request of the authorized Government authority.

6.2 Roles and Responsibilities of CIRT

- Vulnerability Reporting
- Incident Reporting
- Penetration testing
- Incident Analysis
- Vulnerability Assessment of various government Websites
- Log analysis
- Identify and classify cyber-attack scenarios.
- Determine the tools and technology used to detect and prevent attacks.
- Develop a checklist for handling initial investigations of cyber-attacks.
- Determine the scope of an internal investigation once an attack has occurred.
- Conduct any investigations within the determined scope.
- Promote cyber security awareness within departments.
- Address data breach issues, including notification requirements.
- Conduct follow up reviews on the effectiveness of the department's response to an actual attack.
- Prepare SOP for different types of crisis.

7. Strategy and Goals for Cyber Incident Response

Impact Definitions:

Security Objective	Potential Impact		
	Low	Medium	High
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Integrity: Guarding against improper information modification or	The unauthorized modification or destruction of information could be	The unauthorized modification or destruction of information could be	The unauthorized modification or destruction of information could be

destruction, and includes ensuring information nonrepudiation and authenticity.	expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	expected to have a serious adverse effect on organizational operations, organizational assets, or individuals	expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals
Availability: Ensuring timely and reliable access to and use of information	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Timely and thorough action to manage the impact of cyber incidents is a critical component of the response process. The response should limit the potential for damage by ensuring that actions are systematic and coordinated. Cyber incident response goals are:

To protect the well-being of the Government.

- To protect the confidentiality, integrity, and availability of Government systems, networks and data.
- To help Government personnel recover their service processes after computer or network security incidents.
- To provide a consistent response strategy to system and network threats that put Government digital data and systems at risk.
- To develop and activate a communications plan including initial reporting of the incident as well as ongoing communications as necessary.
- To address cyber related legal issues.
- To coordinate efforts with external Computer Incident Response Teams and other regulatory bodies.
- To minimize the Government reputational risk by notifying appropriate Government officials of cyber incidents that may become high profile events and implementing timely and appropriate corrective actions.

8. Protection and resilience of Organization's infrastructure

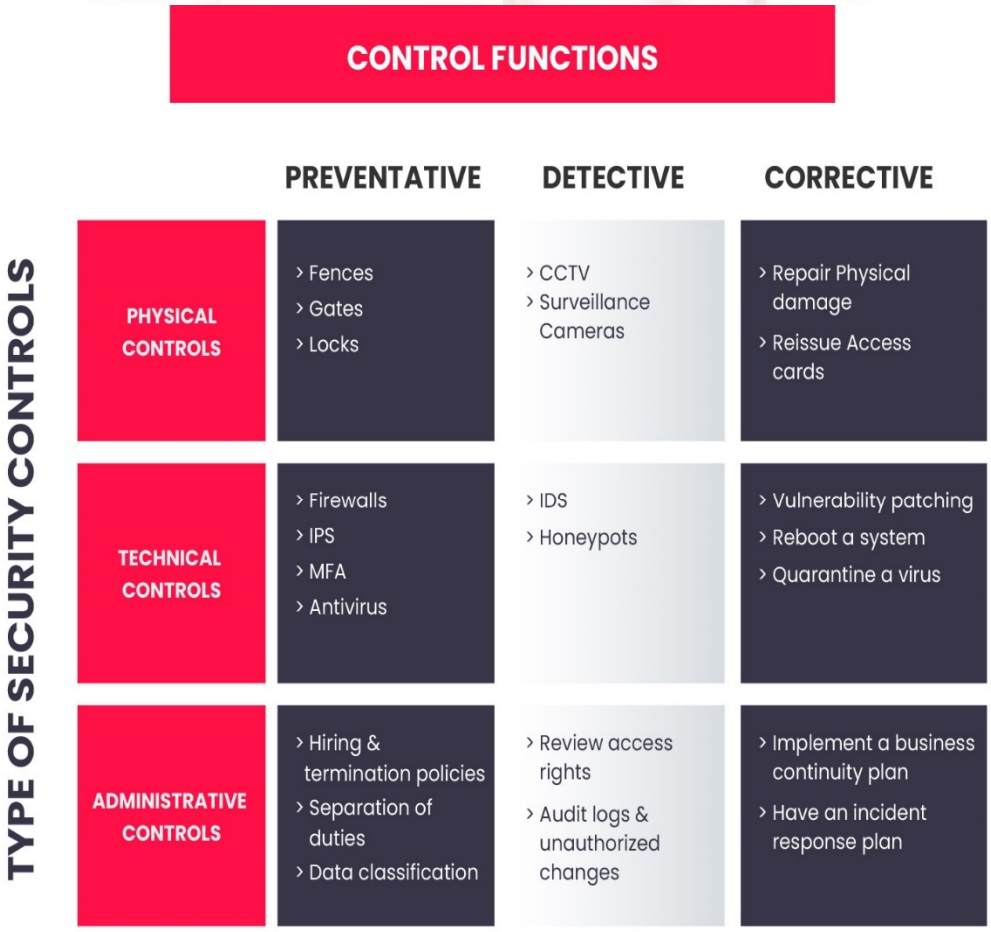
To build cyber resilience, government shall work on the following lines:

- Identification of key information and technology assets that support the services of the organization;
- Implementation of controls to protect those assets from cyber-attack;
- Implementation of controls to sustain the ability of those assets to operate under disruptive events and recover rapidly from disruption;
- Development of processes to maintain and repeatedly carry out the protection and recovery activities;

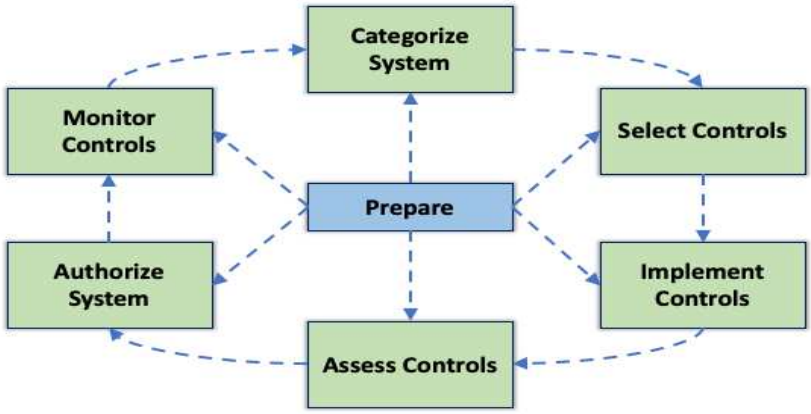
- Development of appropriate measures to drive these activities;
- Development of a plan for protection of organization Infrastructure and its integration with government plan and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.
- To closely interact with MeitY/Cert-IN/NIC by providing the necessary and timely information.
- To ensure identification, prioritization, assessment, remediation, and protection of organization infrastructure and key resources based on the plan for organization Information Infrastructure.

To ensure compliance to global security best practices, government continuity management and cyber crisis management plan by all entities within domain of organization/ department, to reduce the risk of disruption and improve the security posture.

Security Controls function as for protection of organization infrastructure is given below:



Above Controls should be followed with Risk Management Framework as mentioned below:



9. Mock Drills to test preparedness to withstand cyber attacks

Government shall conduct as well as participate in simulated cyber event exercises on their networks and system infrastructure to test their preparedness in respect of response, coordination and recovery mechanism to the simulated cyber security breaches, with the help of CIRT.

9.1 Periodic Mock Drills – Government shall periodically and actively participate in cyber drills conducted under the aegis of Cert-IN, MeitY etc.

The Government shall test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures. Such testing shall also include testing of crisis communication to citizens and other internal and external stakeholders.

10. Reporting a Cyber Incident

A cyber incident is an event that poses a threat to the integrity, availability, or confidentiality of an IT system. Cyber incidents shall be reported immediately to the Chief Information Security Officer or as soon as possible after discovery. All communications regarding cyber incidents must be conducted through channels that are known to be unaffected by the cyber incident under investigation.

Cyber incidents can be reported in several ways including by email, phone, SMS, in-person or by initiating a trouble ticket in Incident Management tool.

Examples of incidents that should be reported immediately include, but are not limited to:

- A virus/worm affecting multiple systems;
- Intrusion or damage to;
    - Web site or page,
    - Computer system or network,
    - Wireless access,
    - Cell phones, smart phones
    - PoS Machine
    - Laptops, tablet computers
    - Fax machines,
    - Voice mail, and
    - Voice over IP (VOIP) systems.

See Annexure -1 & 3 for further guidance on reporting cyber incidents to CIRT, Cert-IN and/ or other controllers.

Early notification allows time to the CISO and affected departments to gather as much information as possible when evaluating potential cyber incidents. Information that should be gathered and shared when reporting cyber incidents includes:

- Contact information of affected individuals
- IP address, hostname, or location of system(s)
- In the case of a website intrusion, the specific URL(s)
- Disclosure of data that may be included on the system. This is particularly important if this data may include Personal Identifiable or Personal Sensitive Information, credit card numbers, account numbers, debit card numbers, driver's license numbers, passport numbers, and medical information.
- Disclosure of the system's criticality, as noted on its most recent IT risk assessment.
- A description of the incident that includes a timeline and identification/detection details.

Prompt reporting may also help reduce common risks associated with cyber incidents, including:

- **Physical safety risk:** As the "Internet of Things" becomes more prevalent in monitoring physical facilities, a cyber-attack against networked devices could cause physical harm to individuals.
- **Regulatory risk:** Compliance with state legislation and regulatory bodies regarding the protection of information. This includes data and systems that fall under IT Act 2023, Indian Companies Act, ISO 27001-2022, ISO 27002-2022, ISO 27005-2022, and state data breach notification laws.
- **Operational risk:** Failure to protect systems and data can cause disruptions to critical daily operations.
- **Financial risk:** Financial Cost may be associated with lost data, restoring systems and data breach notifications.
- **Reputational risk:** There may be a negative impact on confidence in a system or a negative impact on the Government reputation.

11. The Incident Response Processes

This section describes the major phases of the incident response process such as preparation, detection and analysis, containment, eradication and recovery, and post incident activity.

11.1 Preparation

Preparation is fundamental to the success of incident response programs. Incident response methodologies typically emphasize the proactive and ongoing use of tools, training and processes necessary for preventing incidents by ensuring that systems, networks and applications are sufficiently secure. One of the recommended preparation practices for Government departments are to conduct an annual IT Risk assessment. The benefits of conducting an IT Risk Assessment include:

- Identification of applicable threats, including organization-specific threats.
- Categorization and prioritization of each risk to determine if it can be mitigated, transferred or accepted until a reasonable overall level of risk is reached.
- Identification of critical resources and allowing staff to emphasize monitoring and response activities of those resources.

11.2 Identification, Detection, and Analysis

Early steps taken to detect, verify, investigate and analyze an incident are important to develop an effective containment and eradication strategy. Once an incident has been confirmed, resources can be assigned to investigate the scope, impact, and response needed. The detection and analysis phases determine the source of the incident and preserve evidence.

The general steps required for incident identification, detection and analysis are to:

- Review Internal Audit guidelines for department personnel actions with regard to unacceptable computer use and other cyber security incidents.
- Whenever an incident has occurred, coordination between the CIRT and the affected department is important to make sure that steps taken to verify the incident do not alter data that is needed for further investigation.

The CIRT/ IT team will work with the affected department to quickly analyze and validate each incident, keeping the following objectives in mind:

- Identify the root cause(s) of the incident through technical analysis.
- Ensure the accuracy and completeness of incident reports.
- Characterize and communicate the potential impact of the incident.
- Capture the methods used in the attack and the security controls that could prevent future occurrences.
- Research actions that can be taken to respond to and eradicate the

risk and/or threat.

- Understand patterns of activity to characterize the threat and direct protective and defensive strategies.

Technical analysis is iterative in nature. It is conducted many times throughout the incident handling life cycle. Some degree of analysis must occur in order to detect and adequately report an incident. Once an incident has been reported, it may go through several levels of analysis to identify the root cause(s). Each successive level requires personnel those possess more sophisticated skills and have access to additional tools or systems.

The type of analysis conducted will depend on the nature of the incident under analysis. Typically, responding to an incident will require some combination of the following types of analysis:

(1) System Analysis. The process of acquiring, preserving, and analyzing artifacts (e.g., log files or registry information, creating an image, or capturing a screen shot) that help characterize the incident and develop course of action.

(2) Malware Analysis. The process of identifying, analyzing and characterizing reported software artifacts suspected of being adversarial tradecraft to help defense in depth mitigation actions and strategies.

(3) Network Analysis. The process of collecting, examining, and interpreting network traffic to identify and respond to events that violate the security policy or posture of the resources attached to the information network or the network infrastructure and used to support computer security incident investigations. Network incident analysis will include the networks log file to show the threat (e.g., router logs, firewall logs, IDS/IPS logs).

11.3. Forensic Analysis

Computer forensics is considered the application of science to the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody. One model for the forensics process, presented in NIST 800-86, describes four basic phases.

(a) Collection. The first phase in the process is to identify, label, record and acquire data from the possible sources of relevant data, while following guidelines and procedures that preserve the integrity of the data. Collection is typically performed in a timely manner because of the likelihood of losing dynamic data such as current network connections as well as data from battery-powered devices (e.g., cell phones or Personal Digital Assistants).

(b) Examination. Examinations involve forensically processing large amount of collected data. A combination of automated and manual method is used to assess and extract data of particular interest while preserving its integrity.

(c) Analysis. The next phase is to analyze the results of the examination, using

legally justifiable methods and techniques, to derive a conclusion.

(d) Reporting. The final phase is reporting the results of the analysis. This may include describing the methods used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

Guidelines and procedures for forensics evidence collection, handling, and analysis are more extensive and less flexible than those for general incident data collection and analysis. Forensics processing requirements generally exceed typical incident collection and analysis procedures in the following areas:

- Increased preparation and use of specialized tools for acquisition and analysis of evidence.
- Increased level of detail in documenting the scene (e.g., recording model numbers and serial numbers of equipment, photographing hardware, peripherals, wiring and network connections, photographing the monitor/screen, etc.).
- Stricter attention to the order in which volatile system data is acquired (to avoid loss of volatile data).
- Increased care taken to capture persistent data while preventing contamination of evidence (e.g., removing/seizing hard drives and storage media, or creating forensically sound duplicate images on prepared storage devices; using hardware and/or software write blockers to prevent changes to data; and creating hashes of the suspect data and duplicate images to verify authenticity).
- Increased documentation of steps taken during evidence examination and analysis (including date- and time-stamping of all actions taken).
- Increased controls limiting access to evidence and maintenance of a chain of custody.
- Different details to be included in reports of the respective analysis results (different audience).
- Different evidence storage/retention timeframes, policies, and procedures.

11.4. COMMON CATEGORIES OF CYBER INCIDENTS

a) **Targeted Scanning, Probing and Reconnaissance of Networks and IT Infrastructure:** Publicly available reconnaissance techniques, including web and newsgroup searches, WHOIS querying, and Domain Name System (DNS) probing, are used to collect data about the structure of the target network from the Internet without actually scanning the network or necessarily probing it directly.

b) Large scale defacement and semantic attacks on websites: A website defacement is when a Defacer breaks into a web server and alters the contents of the hosted website. Attackers change the content of a web page subtly, so that the alteration is not immediately apparent. As a result, false information is disseminated

c) Malicious Code attacks (virus/worm/ /Trojans/Botnets): Malicious code or malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malicious code is hostile, intrusive, or annoying software or program code. Commonly known malware are virus, worms, Trojans, spyware, adware and Bots

d) Malware affecting Mobile devices: Malicious code and malicious applications (apps) affecting operating systems/platforms used for mobile devices such as Symbian, Android, iOS, Windows Mobile, Blackberry OS

e) Large scale SPAM attacks: Spamming is the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. SPAM mails may also contain virus, worm and other types of malicious software and are used to infect Information Technology systems.

f) Large scale spoofing: Spoofing is an attack aimed at 'Identity theft'. Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage

g) Phishing attacks: Phishing is an attack aimed at stealing the 'sensitive personal data' that can lead to committing online economic frauds. Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication

h) Social Engineering: Art of manipulating people into performing disclosure actions or divulging confidential information

i) Denial of Service (DoS) attacks and Distributed Denial of Service (DDoS) attacks: DoS is an attempt to make a computer resource unavailable to its intended users. A distributed denial of service attack (DDoS) occurs when multiple compromised computer systems flood the communication link (called bandwidth) or resources of a targeted system.

j) Application-Level Attacks: Exploitation of inherent vulnerabilities in the code of application software such as web/mail/databases

k) Infrastructure attacks: Attacks such as DoS, DDoS, corruption of software and control systems such as Supervisory Control and Data Acquisition (SCADA) and Centralized/Distributed Control System (DCS), Gateways of ISPs and Data Networks, Infection of Programmable Logic Control (PLC) systems by sophisticated malware.

l) Compound attacks: By combining different attack methods, hackers could launch an even more destructive attack. The Compound attacks magnify the destructiveness of a physical attack by launching coordinated cyber-attack.

m) Router level attacks: Routers are the traffic controllers of the Internet to ensure the flow of information (data packets) from source to destination. Routing disruption could lead to massive routing errors resulting in disruption of Internet communication.

n) Attacks on Trusted infrastructure: Trust infrastructure components such as Digital certificates and cryptographic keys are used at various levels of cyber space ranging from products, applications and networks.

o) High Energy Radio Frequency Attacks: Use of physical devices like Antennas to direct focused beam which can be modulated from a distance to cause RF jamming of communication systems including Wireless networks leading to attacks such as Denial of Service

p) Cyber Espionage and Advanced Persistent Threats: Targeted attack resulting in compromise of computer systems through social engineering techniques and specially crafted malware.

11.5. Containment, Eradication and Recovery

11.5.1. Containment

Containment procedures attempt to actively limit the scope and magnitude of the attack. Vulnerability in a particular computer architecture can be exploited quickly. Containment involves acquiring, preserving, securing, and documenting all evidence.

Containment has two goals:

11.5.1.1. Prevent data from leaving the network via the affected machines.

11.5.1.1 Prevent attacker from causing further damage to information technology assets.

The CISO assigns a high priority to determining who the attackers are and what vector (port, software vulnerability, etc.) they are using to attack Government hosts. Once this information is obtained, the CISO will request a router block or physical disconnection to temporarily prevent an IP address, port or both from connecting to the Government network. This may disrupt other normal traffic but this disruption will be kept to a minimum. Containing a cyber-incident has a higher priority than maintaining normal business traffic.

The following actions are taken during the containment phase in coordination with the local system administrator.

Possible actions include:

11.5.1.2 Upon direction by the CISO, the local system administrator can proceed to repair the system as needed to return to normal business operations.

11.5.1.3 Securing the physical area on site if necessary.

11.5.1.4 A review of the information provided by the system administrators.

11.5.1.5 Not allowing the system to be altered in any way. Maintaining a low profile in order to avoid tipping off the attacker.

11.5.1.6 Using a trusted system binary kit (Unix/Linux, Windows) to verify the system binaries have not been compromised.

11.5.1.7 Making a forensic copy of the system for further analysis. Ensuring that any backup tapes are in a secure location.

Determine risk of continued operation.

Possible actions include: Disabling network access but leaving the system up. Disabling the port if the attack is ongoing or if the compromised system is attacking another site. The Network Team should utilize available tools to identify and disable the port.

11.5.1.8 Making a recommendation to the IT management (Head of IT, CISO etc.) regarding whether the affected system(s) should remain online. Attempting to restore operations as quickly as possible. However, if the compromised system threatens the integrity of the network or systems connected to the network, it should be disconnected from the net as soon as possible.

11.5.1.9 Changing all user and system credentials on the affected machine(s).

11.5.2 Eradication

Eradication is the removal of malicious code, accounts, or inappropriate access. Eradication also includes repairing vulnerabilities that may have been the root cause of the compromise. A complete reinstallation of the operating system (OS) and applications strongly recommend.

The general steps involved in the eradication phase of incident response are to:

11.5.2.1 Define eradication benchmarks

11.5.2.2 Identify and mitigate all vulnerabilities that were exploited

11.5.2.3 Remove malware, inappropriate materials, and other components

11.5.2.4 If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps to identify all other affected hosts, then contain and eradicate the incident for them

11.5.2.5 Reinstall OS, apply patches, reinstall applications and apply known patches

11.5.3 Recovery

Once the incident has been contained and eradicated, recovery can start. This phase allows government service processes affected by the incident to recover and

resume operations.

The general recovery steps are:

11.5.3.1 Reinstall and patch the OS and applications. Change all user and system credentials.
11.5.3.2 Restore data to the system.
11.5.3.3 Return affected systems to an operationally ready state.
11.5.3.4 Confirm that the affected systems are functioning normally.
11.5.3.5 If necessary, implement additional monitoring to look for future related Post- Incident Activity.

11.5.4 Incident Closure

Documentation of a cyber-incident and the steps taken to mitigate issues encountered are important. The documentation offers an opportunity to improve Incident Response processes and identify recurring issues. Most local issues can be properly documented using the Government IT incident system.

Information about the incident type

11.5.4.1 A description of how the incident was discovered
11.5.4.2 Information about the systems that were affected
11.5.4.3 Information about who was responsible for the system and its data
11.5.4.4 A description of what caused the incident
11.5.4.5 A description of the response to the incident and whether it was effective
11.5.4.6 Recommendations to prevent future incidents
11.5.4.7 A discussion of lessons learned that will improve future responses
11.5.4.8 A timeline of events, from detection to incident closure

Documentation of a cyber-incident and the steps taken to mitigate issues encountered shall be reported to the Board as well as with the other stake holders, controllers and regulators as deemed appropriate.

( ) ( )

Secretary -IT Director - IT

Annexures

Annexure-1: Guidance on Reporting a Cyber Incident

Annexure-2: UT Helpdesk (DNH & DD) for reporting Cyber Incidents.

Annexure-3: Cert-In contacts details for reporting (Central Help Desk).

Annexure-4: Cert-In incident report

1. Security Incident Reporting (SIR) to UT HELPDESK (DNH & DD) (within two to 6 hours):
2. Subsequent update(s) IT Department (updates to be provided if the earlier reporting was incomplete i.e. investigation underway or new information pertaining to the incident has been discovered or as per request of IT Department):

Annexure-1: Guidance on Reporting a Cyber

Incident What to Report

A cyber incident should be reported if it resulted in either:

- Exposure of legally protected data in Government databases, such as citizens information or governments information protected by regulatory bodies

AND/OR

- Major disruption to normal agency activities carried out via the Government data communications, such as network unavailability for all or significant portions of an agency due to a denial of service (DoS) attack.

You should report events that have a real impact on your department. An IT security incident includes, but is not limited to the following events regardless of platform or computer environment, when:

a. Damage is done
b. Loss occurs
c. Malicious code is implanted
d. There is evidence of tampering with data
e. Unauthorized access has been gained or repeated attempts at unauthorized access have been made (from either internal or external sources)
f. There has been a threat or harassment via an electronic medium (internal or external)
g. Access is achieved by the intruder
h. Web pages are defaced
i. A user detects something noteworthy or unusual (a new traffic pattern, new type of malicious code, a specific IP as the source of persistent attacks)
j. There is a denial-of-service attack on the department.
k. Virus attacks adversely affect servers or multiple workstations

l. Other information technology security incidents occur that could undermine confidence and trust in the Government's Information Technology systems.

Annexure-2: UT Helpdesk (DNH & DD) for reporting Cyber Incidents.

	Cyber Cell Dadra Nagar Haveli	Cyber Cell Daman	Cyber Cell Diu
Address	Police Head Quarters, Dadra & Nagar Haveli	Technological & Cyber Criminal Cell(TAC Cell) Office of Suprintendent of Police, Daman, Near State Bank of India, Paanch Rasta, Nani Daman.	SP Office , Fudam, Diu.
Helpline No.	155260		
Contact No.	0260-2642130	0260-2250942/0260-2251104	02875-254441
Email id:	Itcell : dnhp@mha.gov.in Cyber police : dnh@gov.in	phq-dd@gov.in	Ps.diu-dd@nic.in

Annexure-3: Cert-In contacts details for reporting (Central Helpdesk).

Incident Computer Emergency Response Team (Cert-In)

Address : Ministry of Electronics and Information Technology

Government of India, Electronics Niketan,

6, CGO Complex, Lodhi Road, New Delhi – 110 003, INDIA.

- If the query related to cyber security incident, you can report or contact at:
  - Contact: 1800114949
  - Email: incident@cert-in.org.in
  - Fax: 1800116969
- If the query related to vulnerability report, security alert, or any other technical issues/feedback, you can contact at:
  - Ph: 011-22902657 / 1800114949
  - Email: info@cert-in.org.in , advisory@cert-in.org.in , subscribe@cert-in.org.in , csk@cert-in.org.in
  - Fax: 1800116969

Annexure-4: Cert-In incident report form.

Incident Reporting Form

I am: ☐ the effected entity ☐ reporting incident affecting other entity			
Contact Information of the Reporter			
Name & Role/Title	☐ Individual ☐ Organization		
Organization name (if any)			
Contact No.		Email:	
Address:			

Basic Incident Details	
Affected entity (if not same as reporting entity above)	

Incident Type

☐ Targeted scanning/probing of critical networks/systems	☐ Data Breach	☐ Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones
☐ Compromise of critical systems/information	☐ Data Leak	☐ Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning
☐ Unauthorised access of IT systems/data	☐ Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers	☐ Other (Please Specify)
☐ Defacement or intrusion into the website	☐ Attacks or incident affecting Digital Payment systems	----------
☐ Malicious code attacks	☐ Attacks through Malicious mobile Apps	----------
☐ Attack on servers such as Database, Mail and DNS and network devices such as Routers	☐ Fake mobile Apps	
☐ Identity Theft, spoofing and phishing attacks	☐ Unauthorised access to social media accounts	
☐ DoS/DDoS attacks	☐ Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications	
☐ Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks		
☐ Attacks on Application such as E-Governance, E-Commerce etc.		

Is the affected system/network critical to the organization's mission? (Yes / No). (Brief details.)	
Basic Information of Affected System (Provide information that is readily available.)	Domain/URL: IP Address: Operating System: Make/ Model/Cloud details: Affected Application details (If any): Location of affected system (including City, Region & Country): Network and name of ISP:
Brief description of Incident:	Occurrence date & time (dd/mm/yyyy hh:mm): Detection date & time (dd/mm/yyyy hh:mm):

Note: (i) This form provides general guidance in terms of information which could be relevant to the incident.
(ii) It is not mandatory to fill and/or sign this form. Incidents may also be reported by providing relevant information in the communication itself or in any other readable form.
(iii) Reporting entity may, if desired, also provide relevant information other than mentioned in this form.

Mail/Fax incident reports to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in

Annexure- 5: Booklet Cyber Security Awareness for Citizens.