(97)

No: GAD-मातस075/7/2013-DIR-DIT (MH)-DIT (MH)

Directorate of Information Technology,
General Administration Department,
Mantralaya, Mumbai-4000032.
Tel.: 022-22026534
Date: 30/09/2013

Rajesh Aggarwal
Secretary, IT
E-mail – sec.it@maharashtra.gov.in

Subject: Advisory to all Govt. Departments in Maharashtra regarding...

- Hosting of Government Websites, use of Official Email IDs and 1other Cloud Based Services, connecting to NIXI & Sec. 43A Compliance Audits.
- Adoption of Technical Standards for Interoperability Framework and other standards published by GoI for various eGovernance Projects

References:

1. Information Technology Act,2000 as amended in 2008
2. The Public Records Act, 1993
3. Maharashtra State e-Governance Policy 2011
4. Guidelines for Indian Government Websites (GIGW) - NIC & DARPG
5. Email policy (Version 2) of Maharashtra, released on March 1, 2012

Dear Sir / Madam,

I wish to draw your attention towards following issues which assume significance in light of recent incidents which indicate how data kept outside the country is easily accessible to external Governments and their Corporate sector.

A. Website Hosting:

1) DIT in its communication to all departments from time to time, has instructed them to host their websites only on servers located within India. Any website hosting must also comply with CERT-IN guidelines for web security and go through periodic security audits.
2) Guidelines for Indian Government Websites (GIGW) specify that all government websites must use .gov.in or .nic.in domain names. They should NOT USE any other domain names such as .com, .org, .org.in, etc.
3) Section 8.5 of "eGovernance Policy of Maharashtra -2011" which is approved by the Cabinet, states that "All websites and Web-based applications will comply with Website design guidelines issued from time to time by Government of India".
4) Section 4 of the Public Record Acts, 1993 states that "no person shall take or cause to be taken out of India any public records without the prior approval of the Central Government; provided that no such prior approval shall be required if any public records are taken or sent out of India for any official purpose".
5) There have been incidents in recent times, about hackers breaking into government websites e.g. very recently social justice website was hacked, and it was found that this

(98)

website developed and maintained by a private company was running from the United States. Hackers not only deface the government websites, but also tend to steal /manipulate valuable data and even insert malicious content and/or redirect visitor traffic to malicious websites. In case of information leak or hacking of server hosted abroad, there are difficulties investigating the case as Indian laws are difficult to be applied on those agencies.

Considering these issues, it is hereby re-iterated that all websites and Applications of state government departments and all directorates, corporations, public undertakings under them, should be hosted within India and preferably on government owned servers in State Data Centre or NIC data centres or on servers collocated in Tier 3 data centres in India.

B. Use of Official Email ID

1) It has been observed that many government employees use private (i.e. publicly available) email IDs such as Gmail, Yahoo, Hotmail. Several senior government officials in Maharashtra Government have their Gmail/Yahoo/Hotmail IDs listed in government portals as their official email. Through use of such email system, sensitive government data is being transmitted and stored on private servers outside the country. This is clear violation of section 4 of the Public Records Act, 1993, and various other instructions as listed in previous paragraphs.
2) Various Government agencies have been raising concerns over use of email services provided by foreign firms which have their servers located in overseas locations (or nontraceable locations), thus making it difficult to track any misuse or leakages.
3) Department of Electronics and Information Technology, Government of India is drafting a policy on e-mail usage in government offices and departments, which will be released very soon.

In light of all above, all departments are hereby requested that preferably only government provided email IDs, from servers within India, be used for official communication by all government employees. You may contact NIC or DIT or MahaOnline for the same. When Govt. Of India issues any instructions in this regard, they will be brought to the notice of all departments for strict compliance

C. Use of Cloud Based System

While using Gmail, Yahoo, Skype, Evernote, iPad Notes, Google Drive, SkyDrive, Google Docs, Office 365, Dropbox, Amazon cloud, Facebook, Twitter, YouTube, Google Maps etc. same precautions as above would apply regarding sensitive government data or citizen data.

D. Routing traffic through NIXI (National Internet Exchange of India)

SDC hosted in Mumbai is connected to National Internet Exchange of India (NIXI) exchange point at Navi Mumbai. This ensures that domestic Internet packets mostly remain with India. Whenever any department/corporation etc. is hosting a website outside the SDC, or purchasing bandwidth for various locations, it should be ensured that the concerned data centre/ISP is connected to nearby NIXI nodes.

E. Section 43A Compliance Check

Not only security of data, but keeping Citizen's private data secure is also important. Failure to protect sensitive data attracts provisions of Section 43A of Information Technology Act 2000, as amended in 2008. Section 3 of Information Technology

(Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 notified by Govt. Of India on 11th April 2011 defines SPD (Sensitive Personal Data), while Section 8 of these Rules defines Reasonable Security Practices and Procedures. Hence it is advisable that whenever any Department is collecting or keeping Citizen data, Section 43A compliance Audit should be got done.

It is also necessary that appropriate NDA(Non-Disclosure Agreement) is signed with the vendors as well all their employees designing/developing/implementing/maintaining the software, hardware, network, bandwidth etc.

F. Adoption of Technical Standards for Interoperability Framework and other standards published by GoI

As mandated in eGovernance Policy of Government of Maharashta, standards in eGovernance are of a high priority activity. Standards will ensure sharing of information through seamless interoperability of data across e-Governance applications. eGovernance Policy also mandates use of open standards in all e-Governance projects in the state

In view of the above, ensure that all the existing and new e-Governance projects, right from the conceptualization and design stage, should adhere to the listed Technical Standards in Interoperability framework document and other eGovernance standards published by GoI from time to time, which are available at http://egovstandards.gov.in

You are requested to advise all administrative units within your departments, divisional & district offices, directorates, state public undertakings, corporations etc. to comply with this Advisory.

Yours Sincerely,

(Rajesh Aggarwal)

To,

1) All Additional Chief Secretaries/Principal Secretaries/Secretaries of departments
2) All Divisional Commissioners and District Collectors

Copy for favor of information to:

1) Chief Secretary, Government of Maharashtra
2) Secretary DEITY, Government of India
3) DG, CERT-IN
4) DG, NIC Delhi;
5) DDG, NIC Pune;
6) SIO, NIC Mumbai
7) COO, MahaOnline
8) CEO, NIXI