



मध्यप्रदेश राजपत्र

(असाधारण)

प्राधिकार से प्रकाशित

क्रमांक 166]

भोपाल, गुरुवार, दिनांक 25 जून 2026-आषाढ़ 4, शक 1948

गृह विभाग

मंत्रालय, वल्लभ भवन, भोपाल

भोपाल, दिनांक 25 जून 2026

क्रमांक-1326823/3/3/4/0007/2026-B-1-02(गृह); यतः, सूचना प्रौद्योगिकी एवं इलेक्ट्रॉनिक प्रलेखन की उन्नति होने के साथ-साथ न्यायालयों में साक्ष्य के रूप में प्रस्तुत किये जाने वाले इलेक्ट्रॉनिक अभिलेखों की संख्या निरंतर बढ़ रही है;

और यतः, भारतीय नागरिक सुरक्षा संहिता, 2023 (2023 का 46), किसी दृश्य-श्रव्य इलेक्ट्रॉनिक माध्यम से अभिलेखन करने, दस्तावेज अंग्रेषित करने जिसमें इलेक्ट्रॉनिक संचार के माध्यम से अभियोजन प्रसारित करना प्रस्तावित है, साक्ष्य में फोटोग्राफ या वीडियोग्राफी का उपयोग एवं जांच और विचारण में इलेक्ट्रॉनिक तरीके से साक्ष्य के अभिलेखन के लिए उपबंध करती है;

और यतः, भारतीय साक्ष्य अधिनियम, 2023 (2023 का 47) इलेक्ट्रॉनिक अभिलेखों को साक्ष्य के रूप में मान्यता देता है तथा प्राथमिक और द्वितीयक साक्ष्य की ग्राह्यता के लिए उपबंध करता है;

और यतः, यह समीचीन है कि न्यायालयों में इलेक्ट्रॉनिक अभिलेखों को प्राप्त करना, भंडारण, पुनर्प्राप्ति, पहुंच, प्रबंधन एवं परिरक्षण के लिए आपराधिक और सिविल नियम या पद्धति बनायी जाए;

अतएव, भारतीय नागरिक सुरक्षा संहिता, 2023 (2023 का 46) की धारा 530 तथा भारतीय साक्ष्य अधिनियम, 2023 (2023 का 47) की धारा 61, 62 एवं 63 तथा अन्य सामर्थ्यकारी उपबंधों द्वारा प्रदत्त शक्तियों को प्रयोग में लाते हुए, राज्य शासन, मध्यप्रदेश उच्च न्यायालय के परामर्श से, एतद्वारा, न्यायालयों में इलेक्ट्रॉनिक अभिलेख के प्राप्त करने, भण्डारण, पुनर्प्राप्ति, पहुंच प्रबंधन तथा परिरक्षण के लिए निम्नलिखित सामान्य नियम बनाता है, अर्थात्:-

नियम

अध्याय-एक

प्रारंभिक

1. संक्षिप्त नाम, लागू होना और प्रारंभ.-

(1) इन नियमों का संक्षिप्त नाम मध्यप्रदेश इलेक्ट्रॉनिक अभिलेख (न्यायालयों में प्राप्त किया जाना, भंडारण, पुनर्प्राप्ति, पहुंच, प्रबंधन और परिरक्षण) नियम, 2026 है।

- (2) ये मध्यप्रदेश राज्य के भीतर समस्त जिला न्यायालयों और उच्च न्यायालय के अधीनस्थ अन्य न्यायालयों पर लागू होंगे।
- (3) ये मध्यप्रदेश राजपत्र में इनके प्रकाशन की तारीख से प्रवृत्त होंगे।

2. परिभाषाएं.-

(1) इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो,-

- (क) "प्राधिकृत केन्द्र" से अभिप्रेत है, इन नियमों के अधीन इलेक्ट्रॉनिक अभिलेखों को दर्ज करने के लिए उच्च न्यायालय द्वारा अधिसूचित केन्द्र तथा उसमें जिला न्यायालयों में स्थापित ई-सेवा केन्द्र भी सम्मिलित है;
- (ख) "प्राधिकृत कार्मिक" से अभिप्रेत है, इन नियमों के प्रयोजन के लिए उच्च न्यायालय या संबंधित न्यायालय द्वारा नामनिर्दिष्ट या विनिर्दिष्ट व्यक्ति;
- (ग) "कम्प्यूटर आउटपुट" से अभिप्रेत है और इसमें सम्मिलित है, किसी इलेक्ट्रॉनिक अभिलेख में अन्तर्विष्ट कोई जानकारी, जो कागज पर मुद्रित है, ऑप्टिकल या चुंबकीय मीडिया या अर्धचालक मेमोरी में भंडारित, अभिलिखित या कापी की गई है, जो कम्प्यूटर या किसी संचार उपकरण द्वारा प्रस्तुत की गई है या अन्यथा किसी इलेक्ट्रॉनिक रूप से भंडारित, अभिलिखित या कापी की गई है;
- (घ) "डेटा" से अभिप्रेत है, सूचना, ज्ञान, तथ्य, अवधारणाओं या निर्देशों के ऐसे रूपण, जो औपचारिक रूप से तैयार किए जा रहे हैं या किए जा चुके हैं और जिनका किसी कम्प्यूटर प्रणाली या कम्प्यूटर नेटवर्क में किया जाना आशयित है, किया जा रहा है या किया जा चुका है और जो किसी भी रूप में हो सकेगा (जिसमें कम्प्यूटर प्रिंटआउट, चुंबकीय या ऑप्टिकल भंडारण माध्यम, पंचकार्ड, पंच टेप सम्मिलित हैं) या कम्प्यूटर की मेमोरी में आंतरिक रूप से भंडारित किए जाएं;
- (ङ.) "अभिहित सुरक्षित संग्रह" से अभिप्रेत है, इलेक्ट्रॉनिक अभिलेखों को प्राप्त करने, भंडारण, पुनर्प्राप्ति और परिरक्षण करने के लिए उपयोग की गई सुरक्षित संग्रह, जिसमें इन नियमों के अधीन मध्यप्रदेश उच्च न्यायालय द्वारा संधारित या अधिसूचित ई-साक्ष्य संग्रह या कोई अन्य सुरक्षित संग्रह सम्मिलित है;
- (च) "इलेक्ट्रॉनिक उपकरण" से अभिप्रेत है, और इसमें कोई सर्वर, डिजिटल कैमरा, मोबाईल फोन, डेटा कार्ड, पेन ड्राइव अथवा कोई अन्य चुंबकीय, ऑप्टिकल, अर्धचालक, कम्प्यूटर मेमोरी, माइक्रोफिल्म या इसी प्रकार का उपकरण सम्मिलित है, जिसका उपयोग इलेक्ट्रॉनिक डेटा का भंडारण अथवा पारेषित करने के लिए किया जाता है;
- (छ) "इलेक्ट्रॉनिक अभिलेख" से अभिप्रेत है, डेटा, अभिलेख या डेटा जनित, छवि अथवा ध्वनि, जो इलेक्ट्रॉनिक रूप में या माइक्रोफिल्म अथवा कम्प्यूटर जनित माइक्रोचिप के रूप में संग्रहित, प्राप्त अथवा प्रेषित की गई हो;
- (ज) "ई-साक्ष्य प्रणाली" से अभिप्रेत है, अंतर-संचालनीय आपराधिक न्याय प्रणाली पोर्टल जो कम्प्यूटर अनुप्रयोग के माध्यम से अन्वेषण अथवा विचारण के दौरान इलेक्ट्रॉनिक साक्ष्य के संकलन तथा उसके हैश मान के एकीकरण तथा सुरक्षित संग्रह पर उसके परिरक्षण की सुविधा प्रदान करता है;

- (झ) "विशेषज्ञ" भारतीय साक्ष्य अधिनियम, 2023 (2023का 47) की धारा 63 की उप-धारा (4) के खण्ड (ग) के प्रयोजनों के लिए विशेषज्ञ से अभिप्रेत है-
- (एक) कोई व्यक्ति, जिसने कम्प्यूटर अनुप्रयोग, कम्प्यूटर प्रणाली, भंडारण माध्यम, सर्वर, क्लाउड तथा हैश मान एल्गोरिथम में प्रशिक्षण प्राप्त किया हो अथवा शिक्षा अर्जित की हो; या
- (दो) सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) की धारा 79क के अधीन इलेक्ट्रॉनिक साक्ष्य के परीक्षक के रूप में अधिसूचित कोई विभाग, निकाय या अभिकरण; या
- (तीन) इस संबंध में, राज्य सरकार द्वारा, अधिसूचना द्वारा, विनिर्दिष्ट अथवा प्रमाणित कोई अन्य विशेषज्ञ;
- (ज) "उच्च न्यायालय" से अभिप्रेत है, मध्यप्रदेश उच्च न्यायालय;
- (ट) "मिरर इमेज" से अभिप्रेत है, कम्प्यूटर हार्ड ड्राइव की बिट-टू-बिट प्रतिलिपि जिसमें यह सुनिश्चित किया जाता है, कि फॉरेंसिक परीक्षण के दौरान ऑपरेटिंग सिस्टम में कोई परिवर्तन न हो;
- (ठ) "केवल-पठनीय अथवा राइट-ब्लॉकड मोड" से अभिप्रेत है, कोई मोड जिसमें मेमोरी, डेटा अथवा फाइल तक पहुँच संभव हो, किन्तु उपयोगकर्ता द्वारा उसमें कोई संशोधन या विलोपन नहीं किया जा सके;
- (ड) "मान्यताप्राप्त पोर्टल" से अभिप्रेत है, कोई पोर्टल जिसे इन नियमों के अधीन इलेक्ट्रॉनिक अभिलेखों की प्राप्ति या प्रस्तुतिकरण के प्रयोजन के लिए उच्च न्यायालय द्वारा मान्यता प्रदान की गई हो;
- (ढ़) "सुरक्षित संग्रह" से अभिप्रेत है, डिजिटल संग्रह, जिसका सृजन एवं संरक्षण समय-समय पर यथा संशोधित सूचना प्रौद्योगिकी (संरक्षित प्रणाली हेतु सूचना, सुरक्षा प्रथाएं एवं प्रक्रियाएं) नियम, 2018 के अनुरूप हुआ है;
- (ण) "विसंक्रमित वातावरण" से अभिप्रेत है, वह वातावरण, जो धूल मिट्टी, आर्द्रता, तरल पदार्थ, अत्यधिक तापमान, बाह्य विद्युत, नाभिकीय एवं चुंबकीय क्षेत्रों के प्रभाव से संरक्षित हो।
- (2). इन नियमों में, जब तक कि संदर्भ से अन्यथा अपेक्षित न हो, "इलेक्ट्रॉनिक हस्ताक्षर करना", "डिजिटल हस्ताक्षर", "इलेक्ट्रॉनिक प्ररूप", "इलेक्ट्रॉनिक हस्ताक्षर" और यहां प्रयुक्त ऐसे अन्य शब्द एवं अभिव्यक्तियां, जो इन नियमों में परिभाषित नहीं हैं, का वही अर्थ होगा, जो उन्हें सूचना प्रौद्योगिकी अधिनियम, 2000 (2000 का 21) अथवा उसके अधीन बनाए गए नियमों में उनके लिए समनुदेशित किए गए हैं।

अध्याय-दो

इलेक्ट्रॉनिक अभिलेख प्रस्तुतीकरण तथा प्राप्ति

3. (1) उच्च न्यायालय, इन नियमों के अधीन इलेक्ट्रॉनिक अभिलेखों की प्राप्ति, भंडारण, पुनर्प्राप्ति, पहुच, प्रबंधन तथा परिरक्षण के प्रयोजन के लिए एक या से अधिक सुरक्षित संग्रह अधिसूचित करेगा ।
 - (2) पुलिस द्वारा अन्वेषण के दौरान इलेक्ट्रॉनिक साक्ष्य के संग्रहण हेतु उपयोग की जाने वाली ई-साक्ष्य प्रणाली का संग्रह, इन नियमों के अधीन अभिहित सुरक्षित संग्रह समझा जाएगा।
 4. (1) किसी इलेक्ट्रॉनिक अभिलेख में निहित कोई डाटा या सूचना या सामग्री, जिसमें इलेक्ट्रॉनिक हस्ताक्षर द्वारा अभिप्रमाणित विषयवस्तु सम्मिलित है, जिसे इलेक्ट्रॉनिक रूप में न्यायालय के समक्ष प्रस्तुत किया जाना है और/या सिद्ध किया जाना आशयित है, उसे किसी इलेक्ट्रॉनिक उपकरण के माध्यम से प्रस्तुत किया जाएगा या उसे अभिहित सुरक्षित संग्रह को पारेषित करने के लिए मान्यताप्राप्त पोर्टल पर अपलोड किया जाएगा,
 - (2) शासकीय अभिकरण की दशा में, जिसमें पुलिस सम्मिलित है, ऐसे इलेक्ट्रॉनिक अभिलेख, सुरक्षित नेटवर्क के माध्यम से या ऐसे अभिहित सुरक्षित संग्रह को अंतरित किए जा सकेंगे अथवा ऐसे अभिकरण सुरक्षित संग्रह से अंतरित किए जा सकेंगे।
 - (3) यदि मूल इलेक्ट्रॉनिक अभिलेख अथवा किसी इलेक्ट्रॉनिक उपकरण में अंतर्विष्ट कोई कम्प्यूटर आउटपुट न्यायालय में प्रस्तुत किया जाना हो, तो वह पक्षकार द्वारा उपलब्ध कराए गए ऐंटी-स्टैटिक और चुंबकीय प्रभावरोधी लिफाफे में रखा जाएगा। ऐसे लिफाफे पर पक्षकार द्वारा वाद क्रमांक, पक्षकारों के नाम, अभिरक्षा अनुक्रम तथा प्रमाणपत्र, यदि कोई हो, सहित आवश्यक विवरण अंकित किए जाएंगे तथा उसे विसंक्रमित वातारण में रखा जाएगा:
- परन्तु न्यायालय, पक्षकार को उप-नियम (1) के अधीन इलेक्ट्रॉनिक उपकरण में अंतर्विष्ट ऐसे इलेक्ट्रॉनिक डाटा या अभिलेख को प्रस्तुत करने का निर्देश दे सकेगा या विचारण के किसी भी चरण पर उसे अभिहित सुरक्षित संग्रह को अंतरित किए जाने का निर्देश दे सकेगा।
5. कार्यवाही के किसी पक्षकार से भिन्न अन्य कोई व्यक्ति, न्यायालय की पूर्व अनुमति के बिना, मान्यताप्राप्त पोर्टल के माध्यम से अभिहित सुरक्षित संग्रह पर, कोई इलेक्ट्रॉनिक अभिलेख अपलोड नहीं करेगा।
 6. इन नियमों के अधीन इलेक्ट्रॉनिक अभिलेख अपलोड करने की सुविधा का उपयोग, पक्षकारों द्वारा उनके अधिवक्ताओं अथवा प्राधिकृत कार्मिकों के माध्यम से, उच्च न्यायालय द्वारा मान्यताप्राप्त प्राधिकृत केन्द्रों पर किया जाएगा।
 7. मान्यताप्राप्त पोर्टल पर इलेक्ट्रॉनिक अभिलेख प्राप्त होने तथा उसके अभिहित सुरक्षित संग्रह पर अंतरित किए जाने पर, इलेक्ट्रॉनिक अभिलेख के प्रणाली जनित हैश मान को, उसके प्राप्त होने के समय और अन्य आवश्यक गुणधर्मों (जानकारी) सहित अभिलिखित किया जाएगा ।

8. यदि कोई इलेक्ट्रॉनिक अभिलेख, नियम 4 के उप-नियम (1) के अधीन प्रस्तुत किया जाता है, तो अभिलेख का विवरण जिसमें हैश मान, प्राप्ति की तारीख एवं समय, अंतर्विष्ट हो, पक्षकार या उसके अधिवक्ता द्वारा सत्यापित किया जाएगा, जो ऐसे इलेक्ट्रॉनिक अभिलेख के साथ संलग्न की गई पैकेज फाईल का भाग होगा।
9. मान्यताप्राप्त पोर्टल के माध्यम से प्रस्तुत प्रत्येक इलेक्ट्रॉनिक अभिलेख को विशिष्ट पहचान संख्या उपलब्ध की जाएगी। इलेक्ट्रॉनिक अभिलेख से संबंधित विवरण, जिसमें हैश मान, जनित अभिलेख की प्राप्ति का दिनांक और समय सम्मिलित है, को पैकेज फाईल निर्मित करने वाले उस इलेक्ट्रॉनिक अभिलेख का भाग माना जाएगा।
- 10 जहां इलेक्ट्रॉनिक अभिलेख प्रस्तुत करने को कहा गया है, वह पहले से ही सुरक्षित संग्रह में परिरक्षित है और उसकी विशिष्ट पहचान संख्या और अन्य सुसंगत विवरण जिसमें हैश मान, अभिलेख के प्राप्त होने की तारीख और समय सम्मिलित है, तो नियम 8 के अधीन पक्षकार द्वारा उसे सत्यापित करने की आवश्यकता नहीं होगी। ऐसे सर्वर पर, इलेक्ट्रॉनिक अभिलेख की पहचान संख्या नियम 9 के अधीन विशिष्ट पहचान संख्या समझी जाएगी।
11. पैकेज फाईल में अन्य डाटा के साथ विशिष्ट पहचान संख्या वाला इलेक्ट्रॉनिक अभिलेख, न्यायालय की अनुमति से संबंधित मामले के अभिलेख का भाग होगा।
12. सुरक्षित संग्रह पर इलेक्ट्रॉनिक अभिलेख अपलोड करने तथा विशिष्ट पहचान संख्या समनुदेशित करने के पश्चात्, नियम 4 के उप-नियम (1) के अधीन प्रस्तुत किया गया इलेक्ट्रॉनिक उपकरण, यदि कोई हो, तो उसे प्रस्तुत करने वाले पक्षकार या काउंसिल को वापस किया जाएगा।
13. कोई पक्षकार, सुरक्षित संग्रह या मान्यताप्राप्त पोर्टल पर अप्रासंगिक डाटा/ इलेक्ट्रॉनिक अभिलेखों को डंप करते हुए पाया जाता है, तो उसे संबंधित न्यायालय द्वारा दंडात्मक जुर्माना अधिरोपित कर दंडित किया जा सकेगा। न्यायालय, ऐसे इलेक्ट्रॉनिक अभिलेख को हटाने का निर्देश भी दे सकेगा।
14. समस्त मामलों में, जहां इलेक्ट्रॉनिक अभिलेख द्वितीयक प्रकृति का कम्प्यूटर आउटपुट है, तो उसे प्रस्तुत करते समय, भारतीय साक्ष्य अधिनियम, 2023 (2023 का 47) की अनुसूची में विनिर्दिष्ट प्रमाण-पत्र के साथ संलग्न किया जाएगा:

परंतु इसमें अन्तर्विष्ट कोई भी बात, किसी भी पक्षकार को न्यायालय की अनुमति प्राप्त करने के पश्चात्, ऐसा प्रमाण-पत्र बाद में प्रस्तुत करने से नहीं रोकेगा:

परंतु यह और कि इसमें अन्तर्विष्ट किसी भी बात का यह अर्थ नहीं लगाया जाएगा कि मामले की कार्यवाही के दौरान, मूल प्रमाण-पत्र प्रस्तुत करने से पक्षकार को छूट दी जाएगी।

15. (1) जहां इलेक्ट्रॉनिक अभिलेख ऐसी प्रकृति का है कि ऐसे अभिलेख का खुलासा करना निषिद्ध है या पक्षकारों या पीडित के हित में नहीं है, तो इलेक्ट्रॉनिक अभिलेख, न्यायालय की अनुमति से, नियम 4 के अधीन प्रस्तुत किए बिना, न्यायालय में सीधे प्रस्तुत किया जा सकेगा:

परंतु न्यायालय, कारणों को लिखित में अभिलिखित करते हुए, इलेक्ट्रॉनिक अभिलेख को, अन्यथा मान्यताप्राप्त पोर्टल या अभिहित सुरक्षित संग्रह के माध्यम से प्रस्तुत करने की अनुमति दे सकेगा।

- (2) कोई व्यक्ति, जिसके विरुद्ध भारतीय न्याय संहिता, 2023 (2023 का 45) की धारा 64 या 65 या 66 या 67 या 68 या 69 या 70 या 71 के अधीन या किसी अन्य यौन अपराध का आरोप लगाया गया हो या उसे दोषी पाया गया हो, की पहचान का खुलासा करने वाला कोई भी इलेक्ट्रॉनिक अभिलेख नियम 4 के अधीन प्रस्तुत नहीं किया जाएगा।

अध्याय-तीन
न्यायिक कार्यवाहियों में इलेक्ट्रॉनिक अभिलेख
की पहुंच तथा उपयोग

16. (1) इन नियमों के अधीन प्रस्तुत पैकेज फाइल सहित इलेक्ट्रॉनिक अभिलेख की एक प्रति, किसी पक्षकार, पीडित या विधि की मांग करने वाले किसी अन्य व्यक्ति को इलेक्ट्रॉनिक माध्यम से केवल पढ़ने योग्य प्ररूप में उपलब्ध कराया जा सकेगा तथा इसे विधिवत् रूप में उपलब्ध कराया गया माना जाएगा:

परंतु यदि ऐसा इलेक्ट्रॉनिक अभिलेख विशाल या संवेदनशील प्रकृति का है, ऐसे इलेक्ट्रॉनिक अभिलेख की विषयवस्तु का अप्रकटीकरण करना आवश्यक है, तो पक्षकार या पीडित को उसकी प्रति प्रस्तुत करने के बजाय न्यायालय निर्देश दे सकेगा कि पक्षकारों को न्यायालय में केवल व्यक्तिगत रूप से या अधिवक्ता के माध्यम से निरीक्षण करने की अनमति दी जाए।

- (2) अभिहित सुरक्षित संग्रह पर परिरक्षित अन्य पैकेज फाइल सहित ऐसे इलेक्ट्रॉनिक अभिलेख तक पहुंच उपलब्ध कराने वाली किसी लिंक को भी इस संबंध में उपबंध के सम्यक अनुपालन के रूप में माना जाएगा।
17. (1) इन नियमों के अधीन प्रस्तुत पैकेज फाइल सहित कोई इलेक्ट्रॉनिक अभिलेख, यदि कोई हो, साक्ष्य के रूप में प्राप्त किया जा सकेगा तथा अभिहित सुरक्षित संग्रह पर भण्डारित किया जा सकेगा।
- (2) साक्ष्य में स्वीकार किए गए इलेक्ट्रॉनिक अभिलेख तथा पैकेज फाइल विधि के अनुसार पृष्ठांकित की जाएगी तथा न्यायालय, अपनी विशिष्ट पहचान संख्या के संदर्भ में अपने बयान-पत्र या आदेश में अपने इलेक्ट्रॉनिक हस्ताक्षर चरुपा कर सकेगा या इसकी पहचान कर सकेगा। ऐसा इलेक्ट्रॉनिक अभिलेख तथा पैकेज फाइल समस्त प्रयोजनों के लिए अभिलेख का भाग बनेगा।
18. न्यायालय, पक्षकार के आवेदन पर, विशेषज्ञ/फॉरेंसिक जांच के लिए पैकेज फाइलों सहित इलेक्ट्रॉनिक अभिलेख की एक प्रति उपलब्ध कराने या उस तक पहुंच की अनुमति दे सकेगा। ऐसी प्रति तैयार करने का खर्च आवेदन करने वाले पक्षकार द्वारा वहन किया जाएगा।
19. जहां किसी इलेक्ट्रॉनिक अभिलेख को किसी शासकीय पोर्टल पर इलेक्ट्रॉनिक रूप से उपलब्ध कराया जाता है तथा उसकी एक प्रति जिसमें प्रिन्टआउट सम्मिलित है प्रस्तुत किया जाता है, तो न्यायालय इलेक्ट्रॉनिक अभिलेख की प्रमाणिकता तथा ग्राह्यता के रूप में संतुष्ट होने पर, इलेक्ट्रॉनिक अभिलेख से ऐसी प्रति की तुलना कर सकेगा तथा दोनों को साक्ष्य के रूप में प्राप्त कर सकेगा। न्यायालय, इलेक्ट्रॉनिक अभिलेख के स्रोत के ब्यौरे सम्मिलित करते हुए प्रतिलिपि पर उचित पृष्ठांकन करेगा।
20. इन नियमों में की किसी भी बात को विधि के अनुसार इलेक्ट्रॉनिक अभिलेख के प्रमाण के साथ छूट देने के रूप में नहीं समझा जाएगा।
21. साक्ष्य में स्वीकृत इलेक्ट्रॉनिक अभिलेख की एक प्रमाणित प्रति अधिकृत कार्मिक के प्रमाण-पत्र के साथ केवल पढ़ने योग्य (रीड ओनली) या राइट ब्लॉकड मोड में प्रदान की जा सकेगी। ऐसा प्रमाण-पत्र इलेक्ट्रॉनिक अभिलेख का हैश मान प्रदान करेगा तथा ऐसे अधिकृत कार्मिक द्वारा उसके नाम, उनके आधिकारिक शीर्षक के साथ दिनांकित और स्वीकृत किया जाएगा तथा इलेक्ट्रॉनिक रूप से हस्ताक्षरित होगा। ऐसे अधिकृत कार्मिक को यह माना जाएगा कि ऐसा इलेक्ट्रॉनिक अभिलेख उसकी अभिरक्षा में है।

अध्याय-चार
इलेक्ट्रॉनिक अभिलेख का परिरक्षण

22. न्यायालय, अभिलेख का भाग बनने वाले इलेक्ट्रॉनिक अभिलेख को अभिहित सुरक्षित संग्रह में ऐसी अवधि के लिए परिरक्षित किया जाएगा जैसा कि मामले के अभिलेख को नष्ट करने के लिए नियमों में उपबंधित है। इलेक्ट्रॉनिक अभिलेख को ऐसी अवधि के व्यतीत हो जाने के पश्चात् अभिहित सुरक्षित संग्रह से मिटाया जा सकेगा।
23. (1) जहां कोई इलेक्ट्रॉनिक अभिलेख किसी इलेक्ट्रॉनिक उपकरण में प्रस्तुत किया गया है, तो न्यायालय, पक्षकार द्वारा अभिहित संग्रह प्रणाली पर इलेक्ट्रॉनिक अभिलेख पारेषित करने या उसकी प्रमाणिक प्रति प्रस्तुत करने के पश्चात्, इलेक्ट्रॉनिक उपकरण प्रस्तुत करने वाले पक्षकार को वापस कर सकेगा या कारणों को लिखित में अभिलिखित करते हुए उसे अपने पास रखने का निर्देश दे सकेगा।
- (2) न्यायालय, इलेक्ट्रॉनिक उपकरण वापस करने के पहले, उसे प्रस्तुत करने वाले पक्षकार को इलेक्ट्रॉनिक अभिलेख हटाने का आदेश भी दे सकेगा।

अध्याय- पांच
विविध

24. (1) उच्च न्यायालय, समय-समय पर, इलेक्ट्रॉनिक अभिलेखों के लिए तकनीकी मानकों और अभिहित सुरक्षित संग्रह के रखरखाव, सुरक्षा तथा डाटा पुनर्प्राप्ति के लिए दिशानिर्देश जारी कर सकेगा।
- (2) जब तक उच्च न्यायालय द्वारा स्वदेशी, सुरक्षित संग्रह नहीं बनाया जाता है, तो उच्च न्यायालय, इन नियमों के प्रयोजनों के लिए किसी अन्य सुरक्षित संग्रह को मान्यता दे सकेगा, जो समय-समय पर संशोधित सूचना प्रौद्योगिकी (संरक्षित प्रणाली के लिए सूचना, सुरक्षा प्रथाएं और प्रक्रियाएं) नियम, 2018 के अनुरूप होगा।
25. कोई भी व्यक्ति, इन नियमों के अधीन यथा उपबंधित प्रयोजनों के सिवाय किसी अन्य प्रयोजनों के लिए अभिहित सुरक्षित संग्रह पर किसी इलेक्ट्रॉनिक अभिलेख का उपयोग नहीं करेगा।

मध्यप्रदेश के राज्यपाल के नाम से तथा आदेशानुसार,

कृष्णावेणी देशावतु, सचिव.

भोपाल, दिनांक 25 जून 2026

क्रमांक-1326823/3/3/4/0007/2026-B-1-02(HOME) भारत के संविधान के अनुच्छेद

348 के खण्ड (3) के अनुसरण में, इस आशय की समसंख्यक अधिसूचना दिनांक 25 जून 2026 का अंग्रेजी अनुवाद राज्यपाल के प्राधिकार से एतद्वारा प्रकाशित किया जाता है।

मध्यप्रदेश के राज्यपाल के नाम से तथा आदेशानुसार,

कृष्णावेणी देशावतु, सचिव.

Bhopal, the 25th June 2026

F.No.-1326823/3/3/4/0007/2026-B-1-02(HOME); Whereas, Whereas, with the advancement of information technology and electronic documentation, number of electronic records being produced as evidence in Courts are increasing;

and whereas, the Bharatiya Nagarik Suraksha Sanhita, 2023 (46 of 2023) provides for recording through any audio-video electronic means, forwarding of documents, on which the prosecution proposes to rely, through electronic communication, usage of photograph or videography in evidence and recording of evidence in inquiries and trials in electronic mode;

and whereas, the Bharatiya Sakshya Adhiniyam, 2023 (47 of 2023) recognises electronic records as evidence and provides for admissibility of primary and secondary evidence;

and whereas, it is expedient to formulate criminal and civil rules of practice for reception, storage, retrieval, access management and preservation of electronic records in Courts;

now therefore, in exercise of the powers conferred by section 530 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (46 of 2023) and section 61, 62 and 63 of the Bharatiya Sakshya Adhiniyam, 2023 (47 of 2023) and all other enabling provisions, the State Government, in consultation with the High Court of Madhya Pradesh, hereby, makes and issues the following general rules for reception, storage, retrieval, access management and preservation of electronic records in courts, namely:-

RULES

CHAPTER-I PRELIMINARY

1. Short title, application and commencement.-

- (1) These rules may be called the Madhya Pradesh Electronic Records (Reception, Storage, Retrieval, Access Management and Preservation in Courts) Rules, 2026.
- (2) They shall apply to all the District Courts and other Courts sub-ordinate to the High Court, within the State of Madhya Pradesh.
- (3) They shall come into force from the date of their publication in the Madhya Pradesh Gazette.

2. Definitions.-

(1) In these rules, unless the context otherwise requires,-

- (a) “authorized centre” means centre notified by the High Court for filing of electronic records under these rules and it includes e-seva Kendra established at District Courts;
- (b) “authorized personnel” means persons nominated or specified by the High Court or the concerned Court for the purposes of these rules;
- (c) “computer output” means and includes any information contained in an electronic record, which is printed on paper, stored, recorded or copied in optical or magnetic media or semi-conductor memory, which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form;
- (d) “data” means a representation of information, knowledge, facts, concepts or instructions, which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed or has been processed in a computer system or computer network and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
- (e) “designated secured repository” means secured repository used for reception, storage, retrieval and preservation of electronic records, including e-sakshya repository or any other secured repository, maintained or notified by the High Court of Madhya Pradesh under these rules;
- (f) “electronic device” means and includes a server, digital camera, mobile phone, data card, pen drive or any other magnetic, optical, semi-conductor, computer memory, microfilm or similar device used for the purposes of storing or transmitting electronic data;
- (g) “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche;
- (h) “e-sakshya system” means the portal of inter-operable criminal justice system facilitating collection of electronic evidence during investigation or trial through computer application and its hash value integration and preservation on secured repository;

- (i) “expert” for the purposes of clause (c) of sub-section (4) of section 63 of the Bharatiya Sakshya Adhiniyam, 2023 (47 of 2023), means,-
 - (i) any person, who has undergone training or attained education in computer application, computer system, storage media, server, cloud and hash value algorithm; or
 - (ii) any department, body or agency notified as an examiner of electronic evidence under section 79A of the Information Technology Act, 2000 (21 of 2000); or
 - (iii) any other expert, specified or certified by the State Government in this regard, by notification;
 - (j) “High Court” means the High Court of Madhya Pradesh;
 - (k) “mirror image” means a bit-to-bit copy of the computer hard drive that ensures that the operating system is not altered during forensic examination;
 - (l) “read only or write blocked mode” means a mode, wherein memory or data or a file is capable of being accessed but not of being modified or deleted by the user;
 - (m) “recognized portal” means a portal, which is recognized by the High Court for the purposes of reception or presentation of electronic record under these rules;
 - (n) “secured repository” means a digital repository, which is created and secured in consonance with the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, as amended from time to time;
 - (o) “sterile environment” means environment protected from dirt, humidity, fluids, extreme temperatures, external electric, nuclear and magnetic fields.
- 2) In these rules, unless the context otherwise requires, “affixing electronic signature”, “digital signature”, “electronic form”, “electronic signature” and any other word and expressions used but not defined in these rules shall have the same meaning respectively, as assigned to them under the Information Technology Act, 2000 (21 of 2000) or rules made thereunder.

CHAPTER-II**PRESENTATION AND RECEPTION OF ELECTRONIC RECORD**

3. (1) The High Court shall notify one or more secured repository, for the purposes of reception, storage, retrieval, access management and preservation of electronic records under these rules.
- (2) The repository of e-sakshya system used for collection of electronic evidences during investigation by Police shall be deemed to be designated secured repository under these rules.
4. (1) Any data or information or content in an electronic record, including content authenticated by means of electronic signature, that is sought to be produced in Court, in an electronic form and/or intended to be proved, shall be submitted through an electronic device or uploaded on recognized portal to be transmitted designated secured repository.
- (2) In case of Government agencies, including Police, such electronic records may be transmitted to the designated secured repository, through secured network or assessed from the secured repository of such agency.
- (3) If the original electronic record or any computer output contained in electronic device is sought to be produced in Court, it shall be placed in anti-static and magnetic proof envelope, to be provided by the party. Such envelope shall be appropriately labeled by the party with necessary details, including case number, name of parties, sequence of custody and certificate, if any and shall be kept in a sterile environment:

Provided that the Court may also direct the party to submit such electronic data or record contained in electronic device under sub-rule (1) or direct the same to be transmitted to designated secured repository at any stage of the trial.
5. No person other than the party to the proceedings, without prior permission of the Court, shall upload any electronic record through recognised portal, on the designated secured repository.
6. The facility of uploading electronic record under these rules, shall be availed by the party, through their advocates or authorized personnel, at the authorized centers recognized by the High Court.
7. Upon reception of the electronic record on recognized portal and its transmission on designated secured repository, a system generated hash value of the electronic record shall be recorded along with the time of reception and other necessary properties.

8. If any electronic record is produced under sub-rule (1) of rule 4, the details containing hash value, date and time of the reception of record, shall be verified by the party or his advocate, which shall be part of a package file attached along with such electronic record.
9. A unique identity number shall be provided to each electronic record submitted through the recognized portal. The details relating to the electronic record, including hash value, date and time of the reception of record generated, shall be considered part of such electronic record forming a package file.
10. Where the electronic record sought to be produced is already preserved on a secured repository and has unique identity number and other relevant details, including hash value, date and time of reception of the record, it shall not be required to be verified by the party, under rule 8. The identity number of electronic records, on such server, shall be deemed to be the unique identity number under rule 9.
11. The electronic record having unique identity numbers, with other data in package file, shall be part of record of the concerned case with the leave of the Court.
12. After uploading the electronic record on secured repository and assigning the unique identity number, the electronic device produced, if any, under sub-rule (1) of rule 4, shall be returned to the party or counsel producing it.
13. Any party, found to be dumping irrelevant data/electronic records on the secured repository or recognized portal, may be punished with exemplary costs to be imposed by the concerned Court. The Court may also direct removal of such electronic record.
14. In all cases, where the electronic record is a computer output of secondary nature, it shall be accompanied by a certificate specified in the Schedule of the Bharatiya Sakshya Adhiniyam, 2023 (47 of 2023), at the time of submission:

Provided that nothing contained herein shall preclude any party submitting such certificate subsequently, after obtaining leave of the Court:

Provided further that nothing contained herein shall be construed to exempt a party from filing the certificate, in original, during the proceedings of the case.
15. (1) Where the electronic record is of such nature, that disclosure of such record is prohibited or not in the interest of the parties or victim, the electronic record may, with the leave of the Court, be directly presented in the Court, without presentation under rule 4:

Provided that the Court may, for the reasons to be recorded in writing, permit submission of electronic record, otherwise than through recognized portal or designated secured repository.

- (2) No electronic record disclosing identity of any person, against whom an offence under section 64 or 65 or 66 or 67 or 68 or 69 or 70 or 71 of the Bharatiya Nyaya Sanhita, 2023 (45 of 2023) or any other sexual offence is alleged or found to have been committed, shall be presented under rule 4.

CHAPTER-III

ACCESS AND USAGE OF ELECTRONIC RECORD IN JUDICIAL PROCEEDINGS

16. (1) A copy of any electronic record, with packaged files, submitted under these rules, may be furnished to any party, victim or any other person finder law, through electronic means in read only format and shall be considered as duly furnished:

Provided that if any such electronic record is voluminous or sensitive in nature, requiring non-disclosure of the contents of such electronic record, instead of furnishing the party or the victim with a copy thereof, the Court may direct that the parties shall only be allowed to inspect it, either personally or through an advocate in Court.

- (2) Any link providing access to such electronic record with other package files, preserved on designated secured repository, shall also be considered as due compliance of the provision in this regard.
17. (1) Any electronic record with package files, if any, presented under these rules, may be received in evidence and stored on the designated secured repository.
- (2) Electronic record and package files admitted in evidence shall be endorsed as per law and the Court may affix its electronic signatures or identify the same in its deposition sheet or order, with reference to its unique identity number. Such electronic record and package files shall form a part of the record for all purposes.
18. The Court may permit to provide a copy or permit access to the electronic record with package files for expert/forensic examination, on an application by the party. The cost of preparing such copy shall be borne by the party making the application.

19. Where an electronic record is made available in electronic form on any Government portal and a copy thereof, including printout, is produced, the Court may upon satisfaction as to the authenticity and admissibility of the electronic record, compare such copy from the electronic record and receive both in evidence. The Court shall make an appropriate endorsement on copy, including the details of the source of electronic record.
20. Nothing in these rules shall be construed as, dispensing with the proof of the electronic record, in accordance with the law.
21. A certified copy of the electronic record admitted in evidence, may be provided with the certificate of the authorize personnel in read only or write blocked mode. Such certificate shall provide hash value of the electronic record and shall be dated and subscribed by such authorized personnel with his name and official title and shall be electronically signed. Such authorized personnel shall be deemed to have custody of such electronic record.

CHAPTER-IV

PRESERVATION OF ELECTRONIC RECORDS

22. The electronic record forming part of the Court record shall be preserved in the designated secured repository for such period, as the rules for destruction of the case record provides. The electronic record may be erased from the designated secured repository, after the lapse of such period.
23. (1) Where any electronic record is produced in an electronic device, the Court may, after the party transmits the electronic record on designated repository or produces a certified copy of the same, return the electronic device to the party producing it or may direct its retention, for the reasons to be recorded, in writing.
(2) The Court may also order removal of the electronic record, before return of electronic device to the party producing it.

CHAPTER-V
MISCELLANEOUS

24. (1) The High Court may, from time to time, issue guidelines for the technical standards for electronic records and maintenance, protection and data recovery of designated secured repository.
- (2) Until indigenous secured repository is created by the High Court, the High Court may recognize any other secured repository for the purposes of these rules, which is in consonance with the Information Technology (Information Security Practices and Procedures for Protected System) Rules, 2018, as amended from time to time.
25. No person shall use any electronic record on the designated secured repository for the purposes other than as provided under these rules.

By order and in the name of the Governor of Madhya Pradesh,
KRISHNAVENI DESAVATU, Secy.