मध्यप्रदेश शासन की ई-मेल नीति-2014

मध्यप्रदेश शासन

सूचना प्रौद्योगिकी विभाग

मध्यप्रदेश शासन की ई मेल नीति – 2014

1. परिचय

वर्तमान समय में ई-मेल संचार का एक मुख्य साधन है । संचार के इस नए, त्वरित और सर्वव्यापी माध्यम का उपयोग करके मध्यप्रदेश शासन के कार्य को त्वरित गति से, कम खर्च पर विश्वसनीय तरीके से करने के उद्देश्य से यह नीति तैयार की गई है जिसे **मध्यप्रदेश शासन की ई-मेल नीति 2014** कहा जाएगा । संचार के अंतर्गत मध्यप्रदेश शासन के वह आँकड़े (data) आते हैं जो ई-ट्रांजेक्शन के रूप में प्रदेश, देश या संसार में कहीं भी स्थित उपभोक्ता के बीच संचरित होते हैं । यह नीति मध्यप्रदेश शासन द्वारा प्रदत ई-मेल सुविधाओं को वैधानिक स्वरूप प्रदान करने के लिए तथा उनके उपयोग के संबंध में दिशा-निर्देश जारी करती है। मध्यप्रदेश शासन के विभिन्न विभागों तथा उनके आनुसंगी संगठनों,निगमों, मंडलों आदि में कार्यरत कर्मचारियों को, जो इस सुविधा का उपयोग करते हैं, इस ई-मेल नीति का पालन करना अनिवार्य होगा ।

1.1 उद्देश्य

1.1.1 ई-मेल का उपयोग करके मध्यप्रदेश शासन के कार्य को त्वरित गति से, कम खर्च पर विश्वसनीय तरीके से करके आम जनता को लाभ पहुँचाना ।

1.1.2 ई-मेल द्वारा किए गए पत्र व्यवहार / आँकड़ों के संप्रेषण को वैधानिक स्वरूप प्रदान करना ।

1.1.3 मध्यप्रदेश शासन द्वारा प्रदत ई-मेल सुविधा तक उपयोगकर्ताओं की पहुँच व उपयोग सुनिश्चित करना ।

1.1.4 ई-मेल का प्रयोग इलेक्ट्रॉनिक फाईल प्रोसेसिंग की प्रक्रिया के अंग के रूप में करना ।

1.2 कार्यक्षेत्र

1.2.1 मध्यप्रदेश शासन के उन सभी विभागों तथा उनके आनुषंगी संगठनों, सांवैधानिक संस्थाओं, स्वायतशासी संस्थाओं, निगमों, मंडलों, जिन्हें आगे "संगठन" कहा गया है तथा जो अपनी निधि मध्यप्रदेश की संचित निधि से प्राप्त करते हैं, को यह ई-मेल सेवा निःशुल्क प्रदाय की जाएगी ।

1.2.2 मध्यप्रदेश शासन द्वारा प्रदत ई-मेल सुविधा का उपयोग वाले सभी संगठनों के कर्मचारियों पर इस नीति में शामिल दिशा-निर्देश बिना किसी अपवाद के लागू होंगे ।

(सुधीर कुमार कोचर)
उप सचिव
म.प्र. शासन
लोकसेवा विभाग

1.2.3 मध्यप्रदेश शासन द्वारा जारी ई-मेल सुविधा का उपयोग मात्र कार्यालयीन संचार के लिये होगा। अन्य सेवा प्रदायकों द्वारा दी जाने वाली ई-मेल सुविधा का उपयोग कड़ाई से गैर सरकारी / निजी संचार तक सीमित होगा । दूसरे शब्दों में शासकीय कार्य के लिए अनिवार्यत: इसी ई-मेल सेवा का उपयोग करना होगा और इस ई-मेल सेवा पर निजी संचार करने की अनुमति नहीं होगी ।

2. वैधानिक प्रावधान

2.1 इस ई मेल नीति में प्रस्तावित उपबंधों को क्रियान्वित करने के लिए तथा प्रस्तावित ई-मेल सुविधा का उपयोग करते हुए भेजे गए संदेश, आँकड़ों को विधिमान्य बनाने के लिए राज्य शासन, इस नीति के जारी होने के 30 दिन के भीतर, सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 90 में प्रदत शक्तियों का उपयोग करते हुए आवश्यक अधिसूचना जारी करेगा । इसके परिणामस्वरूप ई मेल से प्रेषित जानकारी / पत्र उसी प्रकार मान्य होंगे जैसे कि वे हार्ड कॉपी पर हस्ताक्षर करके भेजे गए हों । ई मेल भेजने के पश्चात पृथक से हार्ड कॉपी पर पुष्टि भेजना आवश्यक नहीं है ।

2.2 मध्यप्रदेश शासन की ई-मेल सेवा प्रारंभ होने तक, सभी विभाग अपने द्वारा प्रदान की गई ई- मेल सुविधाओं को नोडल विभाग के पास प्रविष्ट कराएँगे जो इनकी जानकारी अधिसूचना के रूप में प्रकाशित करेगा । इसके पश्चात उन ई-मेल के उपयोग पर वही निबंधन लागू होना माने जाएँगे जो इस नीति में वर्णित हैं ।

2.3 मध्यप्रदेश शासन की प्रस्तावित सेवा प्रारंभ होने के बाद 3 माह के भीतर सभी संगठन अन्य सेवा प्रदायकों द्वारा प्रदत्त अपनी मेल सुविधाओं का उपयोग बंद कर उसे क्रियान्वयन एजेंसी के केंद्रीकृत परिनियोजन (centralized deployment) पर स्थानांतरित करने की प्रक्रिया प्रारम्भ करेंगे, भले ही वे अपना स्वतंत्र ई-मेल सेट-अप चला रहे हों ।

3. प्रविधि (methodology)

3.1 मध्यप्रदेश शासन, निर्धारित क्रियान्वयन एजेंसी के माध्यम से अपने विभागों व आनुषंगिक संगठनों को समर्पित ई मेल सेवा (dedicated e-mail service) उपलब्ध कराएगा। ई-मेल जैसे संवेदनशील परिनियोजन (sensitive deployment) की सुरक्षा को देखते हुए क्रियान्वयन एजेंसी के माध्यम से परिनियोजित सेवा के अलावा कोई भी अन्य ई-मेल सुविधा मध्यप्रदेश शासन के अधीन नहीं होगी । इस सुविधा का नोडल विभाग सूचना प्रौद्योगिकी विभाग होगा और वही इस सुविधा की क्रियान्वयन एजेंसी के चयन व नियुक्ति के लिए उत्तरदायी होगा । इस नीति के क्रियान्वयन के लिए आवश्यक वैधानिक प्रक्रियाएँ करने / आदेश जारी करने का दायित्व सूचना प्रौद्योगिकी विभाग का होगा। ई मेल सेवा का उपयोग करने के लिए प्रत्येक संगठन नोडल अधिकारी तथा सक्षम प्राधिकारी की नियुक्ति करेगा। ई-मेल सेवा का उपयोग करने के लिए विभिन्न प्रक्रियाएँ इस प्रकार होंगी -

(सुधीर [illegible] श्रीवास्तव)

3.2 <u>अकाउंट निर्माण प्रक्रिया</u>

3.2.1 मध्यप्रदेश शासन की ई मेल सेवा लेने वाले सभी संगठनों के कर्मचारियों को अपना आवेदन पत्र उस संगठन के सक्षम प्राधिकारी को प्रस्तुत करना होगा जो उसकी पूर्ण जाँच उपरांत अनुशंसा सहित क्रियान्वयन एजेंसी भेजेगा । ई-मेल एकाउंट आवंटन का कार्य क्रियान्वयन एजेंसी के द्वारा किया जाएगा ।

3.2.2 आउटसोर्स / संविदा आधार पर कार्यरत अधिकारियों/कर्मचारियों के ई-मेल अकाउंट भी बनाए जा सकेंगे । उनकी प्रक्रिया वही होगी जो उपर बताई गई है परन्तु यह अकाउंट पूर्व निर्धारित समाप्ति तिथि के साथ निर्मित किए जाएँगे । यदि ऐसे अधिकारी/कर्मचारी अनुबंध अवधि समाप्त होने से पूर्व पद त्याग देते है अथवा लंबे समय तक बिना किसी वैध कारण अथवा पूर्व सूचना के अनुपस्थित रहते है तो ऐसी स्थिति में सक्षम अधिकारी द्वारा उक्त संविदाकर्मी की सेवा समाप्त किये जाने की तिथि से उनके ई-मेल अकाउंट निष्क्रिय (Deactivate) कर दिये जावेंगे।

3.2.3 ई-मेल आईडी अधिकारी के नाम तथा पदनाम दोनों के ही आधार पर निर्मित किए जा सकते हैं । पदनाम के आधार पर निर्मित ई मेल आई डी स्थानांतरण/सेवानिवृति के समय पदानुवर्ती अधिकारी को प्रदाय किया जाएगा जबकि नाम के आधार पर निर्मित मेल आई डी आगे दी गई शर्तों के तहत संबंधित अधिकारी अपने पास रख सकेगा ।

3.2.4 मध्यप्रदेश शासन ई-मेल के लिये वर्चुअल डोमेन होस्टिंग की सुविधा मुहैया कराएगा । इस प्रकार यदि कोई उपयोगकर्ता विभाग अपने विभाग का प्रतिनिधित्व करने वाली एड्रेसिंग नीति को अपनाना चाहता है वह तो क्रियान्वयन एजेंसी को आवेदन कर सकता है । तब भी "आई डी" की अद्वित्तीयता (uniqueness) को बनाए रखते हुए संभव होने पर उसे उक्त आईडी प्रदाय किया जा सकेगा ।

3.2.5 क्रियान्वयन एजेंसी से डेलीगेटेड एड्रिमन कंसोल (delegated admin console) की सुविधा प्राप्त करने वाला संगठन इसका उपयोग संबंधित डोमेन के अंतर्गत एकाउंट निर्माण, समाप्ति और यूजर आईडी के पासवर्ड परिवर्तन की प्रक्रिया निर्धारण के लिए आवश्यकतानुसार स्वयं कर सकता है।

3.3 <u>पद आधारित ई-मेल आई डी हस्तांतरण प्रक्रिया</u> :

3.3.1 प्रत्येक अधिकारी अपने त्यागपत्र, सेवानिवृति या स्थानांतरण के समय अपने सक्षम प्राधिकारी के माध्यम से संबंधित नोडल अधिकारी/ क्रियान्वयन एजेंसी को अनिवार्यत: सूचित करेगा । ऐसी सूचना प्राप्त होने पर नोडल अधिकारी/क्रियान्वयन एजेंसी कार्यवाही करेंगे और आधिकारिक एकाउंट का स्टेटस परिवर्तित करेंगे, पासवर्ड को रिसेट करेंगे व उसे पदानुवर्ती अधिकारी को हस्तांतरित करेंगे । उक्त अधिकारी को नोइयूज सर्टिफिकेट देने के पूर्व तथा सेवानिवृति लाभों की प्रक्रिया प्रारंभ करने के पूर्व संबंधित संगठन के लिए यह कार्यवाही करना आवश्यक होगा ।

3.3.2 किसी भी अनाधिकारिक पहुँच से बचाने के लिए ऊपर दी गई प्रक्रिया का पालन अनिवार्य है। अगर किसी आईडी का दुरुपयोग पाया गया तो इसकी जवाबदेही उस संगठन के नोडल अधिकारी की होगी।

3.4 <u>नाम आधारित ई-मेल आई डी की स्थिति में प्रक्रिया</u> :

3.4.1 चूँकि ई मेल किसी भी कर्मचारी के लिए बहुत महत्वपूर्ण पहचान है और वह सभी जगह (जिसमें बैंक एकाउंट, पेंशन एकाउंट आदि शामिल हैं) उपयोग होती है इसलिए उसका निष्क्रिय किया जाना अधिकारियों के लिए असुविधा पैदा करेगा । इस को देखते हुए मध्यप्रदेश शासन के अधिकारियों, जो 20 वर्ष की सेवा के बाद त्यागपत्र देंगे या सेवानिवृत्त होंगे, को उनके व्यक्तिगत नाम से निर्मित ईमेल एकाउंट को रखने की अनुमति होगी । ऐसे अधिकारी की मृत्यु होने की दशा में उक्त विभाग के नोडल अधिकारी की जबावदारी होगी कि वह उसके उत्तराधिकारियों को मृत्यु पश्चात के देय भुगतान करने के पूर्व उस ई मेल एकाउंट को समाप्त कराएँ । प्रत्येक संगठन के सक्षम प्राधिकारी को स्थापना शाखा/पेंशन शाखा के माध्यम से इसकी सूचना क्रियान्वयन एजेंसी तथा नोडल अधिकारी को तत्काल देनी होगी ।

3.4.2 यदि अधिकारी/ व्यक्ति 20 वर्ष की सेवा पूर्ण करने के पूर्व ही त्यागपत्र दे देता है तो उसका निजी एकाउंट अधिकतम 1 वर्ष तक धारण करने की अनुमति होगी । इसी प्रकार अधिकारी की सेवा में रहते मृत्यु हो जाने पर उसके विधिक उत्तराधिकारी को 1 वर्ष तक निजी एकाउंट धारण करने की अनुमति होगी ताकि बैंक एकाउंट, पेंशन एकाउंट आदि के संचालन में कठिनाई न हो । तत्पश्चात उसका एकाउंट समाप्त कर दिया जाएगा । प्रत्येक संगठन के सक्षम प्राधिकारी को स्थापना शाखा/पेंशन शाखा के माध्यम से इसकी सूचना क्रियान्वयन एजेंसी तथा नोडल अधिकारी को तत्काल देनी होगी ।

3.4.3 ई मेल एकाउंट धारण करने से कर्मचारी को किसी प्रकार के पारिश्रमिक की पात्रता नहीं होगी ।

3.5 <u>एकाउंट का निष्क्रियकरण (Deactivation of Accounts)</u>

90 दिन तक एकाउंट का उपयोग न होने पर एकाउंट डिएक्टिवेट हो जाएगा । यदि 180 दिन तक उसे सक्रिय करने का अनुरोध प्राप्त नहीं हुआ तो यूजर आईडी तथा डेटा ई मेल तंत्र से डिलीट हो जाएगा । तत्पश्चात उपलब्ध होने की दशा में, उसी आईडी से एकाउंट पुन: एकाउंट खोलने के लिए सम्पूर्ण औपचारिकताएँ पूर्ण करनीं होंगीं ।

4. <u>उपयोगकर्ता, विभाग तथा क्रियान्वयन एजेंसी की भूमिका</u>

4.1 <u>उपयोगकर्ता की भूमिका</u>

4.1.1 मध्यप्रदेश शासन के ई मेल तंत्र का उपयोग कर प्रेषित किए जाने वाले किसी भी डेटा/ईमेल के लिए उपयोगकर्ता जिम्मेदार होगा । मेल सर्वर से भेजे गए सभी ई मेल्स/डेटा का एकमात्र उत्तरदायित्व उस एकाउंट का स्वामित्व रखने वाले उपयोगकर्ता का होगा । इसलिए उपयोगकर्ता को अपना पासवर्ड किसी अन्य के साथ साझा नहीं करना चाहिए ।

4.1.2 ई-मेल से वर्गीकृत, गोपनीय और निषिद्ध (restricted) श्रेणी के ई मेल भेजने के लिए डिजीटल सिग्नेचर सर्टिफिकेट (DSC) का उपयोग करना अनिवार्य होगा । अधिक गोपनीयता की दृष्टि से ऐसी वर्गीकृत सूचना को इंक्रिप्शन (encryption) और डिजीटल सिग्नेचर के माध्यम से ही भेजा जाना चाहिए ।

4.1.3 अत्यंत गोपनीय श्रेणी में वर्गीकृत की जाने वाली सूचनाओं के संबंध में ई मेल का प्रयोग करने के लिए कि स्टैटिक आई-पी एड्रेस / वर्चुअल प्राईवेट नेटवर्क (VPN)/ वन टाईम पासवर्ड (OTP) का उपयोग किया जाए । इस श्रेणी की सेवाएँ निर्धारित करने का दायित्व संबंधित विभाग के सक्षम प्राधिकारी का होगा ।

4.1.4 उनके उपयोगकर्ता को प्राप्त ईमेल Trash तथा Probable Spam फोल्डर्स से स्वत: ही 7 दिवस में समाप्त (delete) हो जाएँगे । अत: उपयोगकर्ता का दायित्व है कि वह समय समय पर इनकी जॉच करते रहें तथा आवश्यक ई मेल अन्य फोल्डर्स में सुरक्षित रखें । उपयोगर्ता अपने फोल्डर्स, जैसे इनबॉक्स, सेंट मेल या अन्य फोल्डर जो उसने निर्मित किया हो, में सुरक्षित किए गए ईमेल्स के लिए स्वयं उतरदायी होंगे । उपयोगकर्ता द्वारा दुर्घटनावश, जैसे स्थानीय मेल क्लाइंट (Outlook / Eudora / Thunderbird, आदि) के गलत कांफिगरेशन, के कारण डिलीट हो गई ई मेल्स की पुन: प्राप्ति के लिए क्रियान्वयन एजेंसी जिम्मेदार नहीं होगी ।

4.1.5 उपयोगकर्ता कार्यालयीन ई-मेल अकाउंट, जो मध्यप्रदेश शासन के मेल सर्वर पर समनुरूप (Configure) है, को अन्य सेवा प्रदाता के साथ पॉप समनुरूप (POP Configure) करके ई-मेल डाउनलोड नहीं करेंगे ।

4.1.6 उपयोगकर्ताओं को इस बात को खास तौर पर सुनिश्चित करना होगा कि पहुँच हेतु उपयोग में लाई जाने वाली डिवाइसेस (डेस्कटॉप / लैपटॉप / हैंडसेट इत्यादि) में नवीनतम ऑपरेटिंग सिस्टम तथा एप्लीकेशन पैचेज (application patches) हों । उन्हें यह बात भी सुनिश्चित करना होगी कि उक्त डिवाईस में नवीनतम एंटीवायरस सिग्नेचर भी हों।

4.1.7 मध्यप्रदेश शासन द्वारा प्रदत ई-मेल आई.डी. से, सरकारी मेल सेवा से इतर निजी आई.डी. पर मेल स्वत: अग्रेषण (Auto forward/ Mail Divert) करने की अनुमति नही होगी।

4.1.8 शासकीय कर्तव्य पूर्ण करने में उपयोगकर्ताओं को सहायता करने के लिए पेशेगत संसाधन के तौर पर ई मेल प्रदाय की जाती है । इसलिए ई मेल एकाउंट का उपयोग आदर्श रूप से मात्र शासकीय पत्र व्यवहार तक सीमित होना चाहिए ।

4.1.9 सरकारी मेल सुविधा में ऑटो सेव पासवर्ड की अनुमति नहीं होगी और सुरक्षा कारणों से इसे ऑप्शन के रूप में प्रदाय नहीं किया जाएगा ।

4.1.10 सभी उपयोगकर्ताओं को ईमेल सेवा का उपयोग करते समय अपने ईमेल एकाउंट की सुरक्षा के लिए एक सक्षम/स्ट्रॉंग पासवर्ड का उपयोग करना चाहिए | इस संदर्भ में "ईमेल पॉलिसी के अंतर्गत" http://www.deity.gov.in /content/policiesguidelines पर उपलब्ध Password Policy का पालन करना चाहिए ।

4.1.11 प्रत्येक व्यक्ति अपने एकाउंट के लिए, जिसमें उस एकाउंट तक पहुँच (access to the account) की सुरक्षा करना शामिल है, उत्तरदायी होगा । किसी एकाउंट से निर्मित अथवा प्रेषित ई मेल्स, उस एकाउंट धारक द्वारा निर्मित मान्य की जाएँगी ।

4.1.12 उपयोगकर्ता की जिम्मेदारी निम्न बिंदुओं तक विस्तृत होगी -

a. क्लाइंट तंत्र पर की जाने वाली गतिविधियों के लिए वही उपयोगकर्ता जिम्मेदार होगा जिसके नाम पर वह एकाउंट समनुदेशित किया गया है
b. आधिकारिक ई मेल को निजी ई मेल एकाउंट पर अग्रेषित नहीं किया जाएगा ।
c. गलत व्यक्तियों को ई मेल पहुँचने का खतरा कम करने के लिए "रिप्लाइ ऑल" एवं "वितरण सूची" का प्रयोग सावधानी से करना चाहिए ।
d. उपयोगकर्ताओं की नेटवर्क पहुँच, द्वेषपूर्ण तथा अवैधानिक गतिविधियों की मॉनीटरिंग/फिल्टरिंग के अधीन रहेगी ।
e. उपयोगकर्ता को महत्वपूर्ण फाइलों का बैक-अप नियमित अंतराल पर लेना चाहिए। उपयोगकर्ता के क्रियाकलाप के कारण नष्ट हुए डेटा को पुर्नप्राप्त करने का कार्य क्रियान्वयन एजेंसी द्वारा नहीं किया जाएगा।
f. सुरक्षा हादसे की सूचना उपयोगकर्ता, क्रियान्वयन एजेंसी के सिस्टम एडमिनिस्ट्रेटर को देगा।

4.1.13 ई मेल के अनुचित उपयोग के कुछ उदाहरण नीचे दिए गए हैं । उपयोगकर्ताओं को ऐसे कार्य नहीं करना चाहिए -

a. ऐसे ई मेल्स का निर्माण और आदान प्रदान करना जो उत्पीड़क, अश्लील, फूहड़ या धमकी भरे होने की श्रेणी में वर्गीकृत किए जा सकते हों ।
b. मालिकाना या ट्रेडमार्क युक्त जानकारी या अन्य विशेषीकृत, गोपनीय संवेदनशील सूचना का अप्राधिकृत आदान प्रदान करना ।
c. उपयोगकर्ता, सेवा में अप्राधिकृत पहुँच का प्रयास नहीं करेंगे । अप्राधिकृत पहुँच में, उदाहरण के लिए, ई मेल्स का बेनामी बितरण, किसी अन्य अधिकारी का यूजर आईडी उपयोग में लाना या मिथ्या पहचान का उपयोग करना, शामिल है ।
d. विज्ञापन, सामाजिक रूप से भेजे जाने वाले श्रृंखलाबद्ध पत्र, अवांछित ई मेल का निर्माण तथा वितरण ।
e. किसी नियम, जिसमें कॉपीराइट नियम भी शामिल हैं, के उल्लंघन में निर्मित सूचना तथा उसका वितरण ।
f. ऐसी ई मेल, जिसमें कम्प्यूटर वायरस समाहित है, का जानबूझ् कर प्रेषण ।
g. ई मेल प्रेषक की पहचान का गलत निर्वचन ।

h. किसी अन्य व्यक्ति के एकाउंट का उसकी सहमति के बिना प्रयोग करना या प्रयोग करने का प्रयास करना ।

i. धर्म, जाति, वंश, लिंग आदि के संबंध में अपमानजनक भाषा युक्त ई मेल का प्रेषण ।

j. राष्ट्र विरोधी संदेश युक्त ई मेल का आदान प्रदान ।

k. प्रेषण सूची पर व्यक्तिगत ई मेल भेजना । क्रियान्वयन एजेंसी, व्यक्तिगत प्रकृति के ई मेल, जैसे सीजन्स ग्रीटिंग्स, व्यक्तिगत समारोह आदि, भेजने के लिए वितरण सूची का उपयोग करने की अनुमति नहीं देगी ।

l. किसी भी प्रकार का अनुचित उपयोग इस नीति का उल्लंघन समझा जाएगा और अनुशासनात्मक कार्यवाही, जो उचित समझी जाए, की जा सकेगी । इसके अलावा उल्लंघन की प्रकृति के आधार पर जॉच एजेंसियॉ परीक्षण कर सकेंगी ।

4.2 <u>संगठन/विभाग की भूमिका</u> -

मध्यप्रदेश शासन की ईमेल नीति का उपयोग करने वाले प्रत्येक संगठन को निम्नलिखित भूमिका अदा करनी होगी -

4.2.1 हर विभाग में सक्षम प्रधिकारी (Competent authority) की नियुक्ति होगी ।

4.2.2 हर विभाग में पदाभिहित नोडल अधिकारी (Designated nodal officer) होगा ।

4.2.3 सभी संगठन, उपयोगकर्ताओं के लिए ईमेल नीति और उनके विभागीय सेटअप के लिए ई-मेल नीति का पालन सुनिश्चित कराने के लिए, युक्तियुक्त नियंत्रण क्रियान्वित करेंगे ।

4.2.4 संबंधित संगठन यह सुनिश्चित करेंगे कि उनके उपयोगकर्ताओं के आधिकारिक ईमेल एकाउंट केवल सूचना प्रौयोगिकी विभाग द्वारा निर्धारित क्रियान्वयन एजेंसी के मेल सर्वर पर ही निर्मित किए जाएँ ।

4.2.5 उपयोगकर्ताओं को ई मेल नीति से अवगत होना चाहिए । इसलिए विभागों को उपयोगकर्ताओं के स्तर पर ई मेल नीति और उससे संबंधित सभी दस्तावेजों की उपलब्धता सुनिश्चित करना चाहिए । इसके अलावा ईमेल नीति पर समय समय पर प्रशिक्षण और जागरूकता कार्यक्रम आयोजित किए जाने चाहिए । कर्मचारियों के उन्मुखीकरण कार्यक्रम में ई मेल नीति को एक सत्र के रूप में शामिल किया जाना चाहिए ।

4.2.6 संबंधित संगठन का नोडल अधिकारी ईमेल नीति के सुरक्षा पहलुओं से संबंधित सभी घटनाओं का समाधान करना सुनिश्चित करेगा ।

4.2.7 संबंधित संगठन का सक्षम प्राधिकारी यह सुनिश्चित करेगा कि नियमित समयांतरालों पर ई-मेल सुरक्षा प्रशिक्षण कार्यक्रम संचालित होते रहें ।

4.2.8 ऐसी सूचनाएँ जो अत्यंत गोपनीय श्रेणी में वर्गीकृत की जातीं हैं के संबंध में यह अनुशंसित किया जाता है उनके संबंध में ई-मेल का प्रयोग करने के लिए कि स्टैटिक आई-पी एड्रेस / वर्चुअल प्राईवेट नेटवर्क (VPN)/ वन टाईम पासवर्ड (OTP) का

उपयोग किया जाए । इस श्रेणी की सेवाएँ निर्धारित करनें का दायित्व संबंधित विभाग के सक्षम प्राधिकारी का होगा ।

4.2.9 नीति के उल्लंघन की दशा में, संगठन के प्राधिकृत अधिकारी का यह दायित्व होगा कि वह क्रियान्वयन एजेंसी को सूचित करे । यदि ऐसी सूचना नहीं भेजी जाती या विलम्ब से भेजी जाती है तो ऐसी स्थिति में एकाउंट का दुरुपयोग होने या निर्दिष्ट एजेंसी की जॉच के अधीन आने के लिए विभाग जिम्मेदार होगा ।

4.2.10 इस नीति का नोडल विभाग अर्थात् सूचना प्रौद्योगिकी विभाग निर्धारित क्रियान्वयन एजेंसी से ई-मेल सुविधा के स्तर को बनाए रखने हेतु सर्विस लेवल एग्रीमेंट (SLA) करेगा । इसमें वे सभी आवश्यक उपाय किए जाएँगे जो सेवा के अवाधित और प्रभावी उपयोग हेतु आवश्यक हैं ।

4.3 <u>क्रियान्वयन एजेंसी की भूमिका</u>

4.3.1 क्रियान्वयन एजेंसी सेवा स्तर अनुबंध (SLA) के आधार पर ई-मेल सेवा उपलब्ध कराएगी।

4.3.2 ई-मेल एड्रेस का आवंटन करना क्रियान्वयन एजेंसी का कार्य होगा । तारतम्यता बनाए रखने के उद्देश्य से, पूर्व से प्रचलित सभी ई-मेल एड्रेसेज यथावत रखने के हर संभव प्रयास किए जाएंगे । जब कभी भी तकनीकी तौर पर सम्भव होगा, डाटा स्थानांतरण भी किया जाएगा । परन्तु किसी भी अपरिहार्य कारण से ऐसा न कर पाने की दशा में क्रियान्वयन एजेंसी को जिम्मेदार नहीं ठहराया जा सकेगा ।

4.3.3 क्रियान्वयन एजेंसी द्वारा सभी ईमेल का डाटा बैक अप नियमित समयांतराल पर लिया जायेगा ताकि तंत्र के फेल होने/क्रेश होने/ लॉस होने की स्थिति में समय पर डेटा की पुर्नप्राप्ति (recovery) सुनिश्चित की जा सके।

4.3.4 क्रियान्वयन एजेंसी द्वारा ई मेल गेट वे पर ही स्पाम फिल्टर और एंटी वायरस फिल्टर समनुरूप (configure) किए जाएँगे । यह फिल्टर ई मेल तंत्र को वायरस और अवांछित ईमेल से सुरक्षा प्रदान करते हैं । क्रियान्वयन एजेंसी इन फिल्टर्स को नियमित रूप से अपडेट करेगी।

4.3.5 सुरक्षा कारणों से निजी प्रोफाईल के अन्तर्गत वर्तमान मोबाईल नंबरों को अपडेट करना अनिवार्य है। इन नंबरों का प्रयोग क्रियान्वयन एजेंसी द्वारा केवल सुरक्षा संबंधी चेतावनी और सूचना भेजने के लिये किया जाएगा । क्रियान्वयन एजेंसी के लिये मोबाईल नंबरों के अतिरिक्त निजी ई-मेल आई.डी. भी अपडेट करना आवश्यक है जिसका प्रयोग उपभोक्ताओं तक एलर्ट पहुंचाने के लिये एक वैकल्पिक माध्यम के रूप में किया जाएगा।

4.3.6 कोई भी ई-मेल, जो ऐसे उपयोगकर्ता के संबोधित है, जिसका अकाउंट निष्क्रिय अथवा समाप्त कर दिया गया है, को ई-मेल अन्य पते पर अनुप्रेषित (re-direct) नहीं किया जाएगा।

4.3.7 सुरक्षा ढांचे के अंग के रूप में यदि किसी ई-मेल एड्रेस में कोई कमी पाई जाती है, तो उपयोगकर्ता को रजिस्टर्ड मोबाईल नम्बर पर एक एस.एम.एस. एलर्ट भेजा जाएगा। यदि किसी ई-मेल के पासवर्ड के साथ धोखाधड़ी के प्रयास (attempt to

compromise the password) की जानकारी पता चलती है तो भी ई-मेल एलर्ट भेजा जाएगा । ई-मेल तथा एस.एम.एस. दोनों में ही उपयोगकर्ता द्वारा की जाने वाली गतिविधियों का विवरण होगा । यदि कोई उपयोगकर्ता 5 एस.एम.एस. एलर्ट (जो किसी कमी को दर्शा रहे हैं) के बाद भी आवश्यक कदम नहीं उठाता है, तो क्रियान्वयन एजेंसी संबंधित आई.डी. पर पासवर्ड रिसेट करने का अधिकार अपने पास सुरक्षित रखेगी।

4.3.8 ऐसी परिस्थिति में, जब किसी ई-मेल आई डी की सुरक्षा में कमी ई-मेल सर्विस / डाटा की सुरक्षा पर प्रभाव डालने लगे अथवा किसी प्राधिकृत जाँच एजेंसी से ऐसी जानकारी प्राप्त हो, तब क्रियान्वयन एजेंसी उस उपयोगकर्ता आई डी के लिए नया पासवर्ड सेट करेगी। यह कार्य तात्कालिक तौर पर किया जाएगा और संबंधित उपभोक्ता को इसकी सूचना (फोन अथवा एस.एम.एस.) द्वारा बाद में दी जाएगी।

4.3.9 क्रियान्वयन एजेंसी शिकायतों के पंजीयन और ऑनलाइन सहायता प्रदान करने के लिए 24X7 सहायता प्रकोष्ठ का संचालन करेगी । शिकायत के पंजीयन के पश्चात शिकायतकर्ता को एक टिकिट जारी किया जाएगा और समस्या के निराकरण का अनुमानित समय दिया जाएगा।

4.3.10 शिकायतें क्रियान्वयन एजेंसी को मेल भेजकर भी दर्ज कराने की व्यवस्था की जाएगी।

4.3.11 ई-मेल उपयोग हेतु संधारित किये जा रहे मेल सर्वर सभी नवीनतम प्रचलित ब्राउजर्स से Compatible होंगे ताकि उपयोगकर्ता ई-मेल को विभिन्न Devises पर Access कर सकें।

5. अनुशंसित उत्कृष्ट प्रक्रियाएँ (Best Practices)

5.1 ई-मेल एकाउंट एक्सेस करते समय, इस हेतु निर्मित एप्लीकेशन का उपयोग करते हुए, सभी उपयोगकर्ताओं को अपना आखिरी लॉग ईन डिटेल अवश्य चेक करना चाहिए।

5.2 किसी भी वर्गीकृत, गोपनीय और सीमित श्रेणी के ई मेल भेजने के लिए इंक्रिप्शन और डिजिटल सिग्नेचर सर्टिफिकेट का उपयोग करना चाहिए।

5.3 संवेदनशील कार्यालयों में कार्य करने वाले उपयोगकर्ताओं को सुरक्षित प्रमाणीकरण के लिए वन टाइम पासवर्ड (OTP) का उपयोग करना अनिवार्य होगा ।

5.4 उपयोगकर्ताओं को निर्धारित समयावधि पश्चात या नीति के अनुसार अपना पासवर्ड बदलना आवश्यक है।

5.5 अधिक समय के लिये अपने कम्प्यूटर से दूर जाने पर अपने ई-मेल को लॉग-आउट अवश्य करें।

5.6 कार्यालयीन ई-मेल एड्रेस का उपयोग किसी असुरक्षित/फेक वेबसाईट के लिए न करें । ऐसी वेबसाइटें आपके ई मेल इनबॉक्स को भर सकतीं हैं या स्पामर्स थोक में स्पाम (spam) भेज सकते हैं जिनमें वायरस हो सकते हैं ।

5.7 उपयोगकर्ता को हमेशा इंटरनेट ब्राउजर के नवीनतम संस्करण का प्रयोग करना चाहिए।

5.8 "सेव पासवर्ड" और ब्राउजर का "ऑटो कम्प्लीट फीचर्स" अशक्त (disabled) होना चाहिए ।

5.9 दुर्भावनापूर्ण सामग्री के प्रभाव से बचने के लिए इंटरनेट से डाउनलोड की जाने वाली या किसी अन्य पोर्टेबल डिवाईस से कॉपी की जाने वाली फाइलों को उपयोग करने से पूर्व स्कैन अवश्य करना चाहिए ।

5.10 जहाँ भी संभव हो डाउनलोडेड फाईलों की सत्यता (integrity) सुनिश्चित करने के लिए डिजिटल सिग्नेचर / हैश वैल्यू की जाँच अवश्य की जानी चाहिए ।

5.11 किसी भी एस.एस.एल. सर्टिफिकेट को अपनाने से पहले उसकी प्रमाणिकता की जाँच अवश्य करनी चाहिए। हमेशा पूरा यूआरएल टाईप करना चाहिए । मेल में दिये गए लिंक को क्लिक करने से बचना चाहिए। फिशिंग के प्रयासों से बचने के लिये यह अनिवार्य है।

5.12 क्रियान्वयन एजेंसी, ई-मेल द्वारा लॉगिन आई.डी. और पासवर्ड जैसे विवरण की मॉग नहीं करती है। उपयोगकर्ता को चाहिए कि वह ऐसे विवरण की मॉग करने वाले किसी भी ई मेल की उपेक्षा कर दे तथा ई मेल पर किसी के साथ भी ऐसी जानकारी साझा न करे ।

5.13 वेब बेस्ड एप्लीकेशन पर काम पूर्ण करने के पश्चात ब्राउजर सेसन बंद किया जाना चाहिए। ब्राउजर सेसन बंद करने के पूर्व उपयोगकर्ता को वेब बेस्ड सेवाएँ जैसे वेब बेस्ड ई-मेल से लॉग आउट हो जाना चाहिए ।

5.14 दुर्भावनापूर्ण सामग्री(malicious content) भेजने के लिए हैकर द्वारा सामान्य रूप से अपनाया जाने वाला तरीका दूषित संलग्नक (infected attachment) युक्त ई मेल भेजना है, इसलिए यह आवश्यक है कि यूएसबी ड्राइव, सीडी और डीवीडी से होने वाले संक्रमण को रोकने के लिए कम्प्यूटर पर एंटी वायरस सॉफ्टवेयर का उपयोग आवश्यक रूप से किया जाए । यह भी सुनिश्चित करना आवश्यक है कि स्थापित सभी सॉफ्टवेयर के लिए डेस्कटॉप ऑपरेटिंग सिस्टम में नवीनतम ऑपरेटिंग सिस्टम पैचेज उपयोग में लाए जाएँ । ऐसे एंटीवायरसों को नियमित रूप से अपडेट किया जाना चाहिए । सभी संलग्नकों को डाउनलोड करने / क्रियान्वित करने के पूर्व एंटी वायरस प्रोग्राम के द्वारा स्कैन किया जाना चाहिए भले ही वे विश्वसनीय स्रोत से प्राप्त हुए हों ।

5.16 स्पाम के रूप में पहचाने गए ई मेल्स को, उपयोगकर्ता के मेलबॉक्स में स्थित "संभावित स्पाम (Probably Spam)" फोल्डर में प्रेषित किया जाएगा । इसलिए उपयोगकर्ताओं को "संभावित स्पाम" फोल्डर की जाँच प्रतिदिन करना चाहिए ।

5.17 उपयोगकर्ता को चाहिए कि वह ई मेल की प्रकृति के बारे में सुनिश्चित होने के बाद ही संलग्नक को खोले/ ओपन करे । किसी भी प्रकार के संदेह की स्थिति में उपयोगकर्ता को प्रेषक से सपर्क करके ई मेल और/या संलग्नक की सत्यता प्रमाणित कर लेनी चाहिए ।

6. अन्य

6.1 ईमेल की छटनी/ लॉग्स जारी करना : -

6.1.1 उपरोक्त अनुबंधों में किसी भी बात के होते हुए भी, ICERT, NTRO और मध्यप्रदेश शासन / भारत सरकार द्वारा इस कार्य के लिए अधिकृत अन्य Agency, आपवादिक परिस्थितियों में, राष्ट्रीय सुरक्षा से संबंधित या अन्य नीतियों का दुरुपयोग या उल्लंघन होने के मामलों में, क्रियान्वयन एजेंसी से ई मेल/लॉग और पत्रव्यवहार की मॉग कर सकती है|

6.1.2 ऐसी एजेंसियों से प्राधिकृत चैनल से मॉग प्राप्त होने पर क्रियान्वयन एजेंसी आवश्यक सहयोग प्रदान करेगी । इस संबंध में उपयोगकर्ता की सहमति नहीं ली जाएगी ।

6.1.3 क्रियान्वयन एजेंसी किसी भी अन्य संगठन से ईमेल/लॉग की जानकारी प्रदान करने के अनुरोध को स्वीकार नहीं करेगी।

6.2 सुरक्षा संबंधी घटनाओं के प्रबंधन की प्रक्रिया -

6.2.1 सुरक्षा संबंधी घटनाओं का पता लगाने, हानि और क्षति को कम करने और कमजोरियों को दुरुस्त करने के लिए सुरक्षा संबंधी हादसों या घटनाओं की प्रतिक्रिया तथा प्रबंधन (incident response and management) आवश्यक है जिसका उपयोग करके समय पर सूचना को पुनर्स्थापित किया जा सके । यह प्रक्रिया उपयोगकर्ता या प्रशासक द्वारा किए जाने वाले सभी नीतिगत उल्लंघनों पर भी लागू होगी ।

6.2.2 ई मेल सेवा के किसी फीचर, यदि वह तंत्र की सुरक्षा के लिए खतरा प्रतीत होता है या खतरा बन सकता है, को निष्क्रिय या समाप्त करने के सभी अधिकार क्रियान्वयन एजेंसी के पास सुरक्षित रहेंगे ।

6.2.3 भारत सरकार की साइबर सुरक्षा नीति में दिए गए निर्देशों के तहत ऐसी कोई घटना तत्काल आईसीईआरटी और क्रियान्वयन एजेंसी के ध्यान में लाई जानी चाहिए ।

6.2.4 कोई भी विपरीत घटना जो ईमेल सेवा के किसी भी भाग में घटती है और जो डेटा को प्रभावित करती है को सुरक्षा घटना के रूप में परिभाषित किया जाता है, जिसके परिणामस्वरूप -

a. उपयोगकर्ता के एकाउंट को खतरा हो सकता हो ।
b. इस नीति का उल्लंघन होने के कारण सुरक्षा भंग हो सकती हो ।
c. शासकीय डेटा संधारित करने वाला पोर्टबल स्टोरेज मीडिया नष्ट हो सकता हो।
d. मध्यप्रदेश शासन की ईमेल सेवा पर फिशिंग साइट का पता चलता हो ।
e. स्पाम और वायरस का फैलाव जो तंत्र और सेवा को प्रभावित कर सकता हो।
f. ईमेल सेवा की सुरक्षा को प्रभावित करने वाले अन्य परिणाम ।

7. पुनरावलोकन / नीति में संशोधन का प्रावधान

7.1 वर्ष में एक बार या सूचना प्रौद्योगिकी के परिवेश में परिवर्तन होने पर, जो भी पहले हो, या शासन की जरूरतों या अन्य किसी भी अन्य कारण से इस नीति का पुनरावलोकन करने का अधिकार सूचना प्रौद्योगिकी परियोजनाओं की समीक्षा हेतु मुख्य सचिव की अध्यक्षता में गठित साधिकार समिति को होगा। पुनरावलोकन निम्न मूल्यांकन करने के लिए किया जाएगा -

a खतरे के परिदृष्य पर पड़ने बाले प्रभाव का मूल्यांकन - जो कि उपयोग की जा रही तकनीकी/ई-मेल आर्किटेक्चर, नियामक और/या वैधानिक आवश्यकताओं में परिवर्तन होने के कारण होगा परन्तु यह सूची इन्हीं तक सीमित नहीं होगी।

b. नीति में दिए गए सुरक्षा नियंत्रणों की प्रभावोत्पादकता का मूल्यांकन।

---00---