रजिस्ट्री सं० डी० एल०-33004/99 REGD. NO. D. L.-33004/99

भारत का राजपत्र
The Gazette of India

असाधारण
EXTRAORDINARY
भाग I—खण्ड 1
PART I—Section 1
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं. 44] नई दिल्ली, बृहस्पतिवार, फरवरी 19, 2015/माघ 30, 1936
No. 44] NEW DELHI, THURSDAY, FEBRUARY 19, 2015/MAGHA 30, 1936

संचार और सूचना प्रौद्योगिकी मंत्रालय

(इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग)

अ धसूच ा

नई दिल्ली, 18 फ़रवरी, 2015

विषय : भारत सरकार की ई-मेल नीति।

फा. सं. 2(22)/2013-ईजी-II.— 1. प्रस्तावना

1.1 सरकार में संचार के लिए ई-मेल का इस्तेमाल एक प्रमुख साधन के रूप में किया जाता है। संचार में भारत सरकार का ऐसा डेटा शामिल होता है जो देश और विदेश में मौजूद प्रयोक्ताओं [1] के बीच ई-मेल लेन-देन के भाग के रूप में भेजा और प्राप्त किया जाता है ।

1.2 भारत सरकार की इस नीति में ई-मेल सेवाओं के इस्तेमाल के संदर्भ में दिशानिर्देश दिए गए हैं । भारत सरकार की ई-मेल सेवाओं के लिए कार्यान्वयन एजेंसी (आईए) [2] इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग (डीईआईटीवाई), संचार और सूचना प्रौद्योगिकी मंत्रालय के अधीन राष्ट्रीय सूचना विज्ञान केंद्र (एनआईसी) होगी । वे संगठन, जिन्हें ''भारत सरकार की ई-मेल नीति'' के खंड 14 के अंतर्गत छूट प्रदान की गई है, इस नीति के प्रयोजन से कार्यान्वयन एजेंसी (आईए) हो जाएंगे।

2. कार्यक्षेत्र

2.1 उन संगठनों, जिन्हें ''भारत सरकार की ई-मेल नीति'' के खंड 14 के अंतर्गत छूट प्रदान की गई है, को छोड़कर सरकारी पत्राचार के लिए एनआईसी, भारत सरकार की कार्यान्वयन एजेंसी द्वारा प्रदान की जाने वाली ई-मेल सेवाओं का ही इस्तेमाल किया जाएगा । अन्य सेवा प्रदाताओं द्वारा उपलब्ध कराई गई ई-मेल सेवाओं का इस्तेमाल किसी सरकारी पत्राचार के लिए नहीं किया जाएगा ।

2.2 यह नीति भारत सरकार (जीओआई) के सभी कर्मचारियों और उन राज्य/संघ राज्य सरकारों के कर्मचारियों के लिए लागू हैं जो भारत सरकार के साथ-साथ राज्य/ संघ राज्य सरकारों की ई-मेल सेवाओं का इस्तेमाल करते हैं और भविष्य में इस नीति को अपनाने का विकल्प चुनते हैं । इस नीति में निहित निर्देशों का उनके द्वारा अनिवार्य रूप से अनुपालन किया जाना चाहिए इसके लिए कोई अपवाद या छूट नहीं है । ई-मेल सेवाओं के सभी प्रयोक्ता "ई-मेल नीति" शीर्षक के अंतर्गत http://www.deity.gov.in/content/policiesguidelines पर उपलब्ध सहायक नीतियों से आगामी सूचना प्राप्त कर सकते हैं।

2.3 ई-मेल का इस्तेमाल भारत सरकार में इलेक्ट्रॉनिक फाइल संसाधन के एक भाग के रूप में किया जा सकता है । इस संदर्भ में अतिरिक्त सूचना http://darpg.gov.in/darpgwebsite_cms/Document/file/CSMeOP_1st_Edition.pdf पर उपलब्ध है।

3. उद्देश्य

3.1 इस नीति का उद्देश्य यह सुनिश्चित करना है कि सरकारी ई-मेल सेवाओं का इसके प्रयोक्ताओं द्वारा सुरक्षित अभिगम और इस्तेमाल किया जाए। प्रयोक्ताओं की यह जिम्मेदारी होगी कि वे इन संसाधनों का इस्तेमाल दक्षतापूर्वक, प्रभावी ढंग से, विधिमान्य और सैद्धांतिक ढंग से करेंगे । भारत सरकार की ई-मेल सेवा के इस्तेमाल का आशय यह है कि प्रयोक्ता ने इस बात के लिए करार किया है कि उसके लिए यह नीति लागू होगी।

3.2 केंद्र और राज्य/संघ राज्य सरकारों दोनों के मंत्रालयों/विभागों/सांविधिक निकायों/स्वायत्त निकायों (यहां से आगे इस नीति में जिन्हें "संगठन [3]" के रूप में संदर्भित किया गया है, के सभी अधिकारियों को ई-मेल सेवा के अंतर्गत सभी सेवाएं निःशुल्क उपलब्ध कराई जाती हैं। इस संदर्भ में और अधिक सूचना "ई-मेल नीति" शीर्षक के अंतर्गत http://www.deity.gov.in/content/policiesguidelines पर उपलब्ध "एनआईसी की मेल सेवाएं और उपयोग नीति" में उपलब्ध हैं।

3.3 ई-मेल के संदर्भ में जारी की गई अन्य नीतियों, दिशानिर्देशों अथवा अनुदेशों का यह नीति अधिक्रमण करेगी।

4. नीति के कार्यान्वयन हेतु विनिर्दिष्ट भूमिकाएं

भारत सरकार की ई-मेल सेवा के इस्तेमाल हेतु प्रत्येक संगठन की निम्नलिखित भूमिकाएं विनिर्दिष्ट की जाती हैं। कार्य के लिए चिह्नित अधिकारी संगत डोमेने के अंतर्गत कंफिगर किए गए संपूर्ण प्रयोक्ता आधार हेतु जिम्मेदार होगा।

4.1 प्रत्येक संगठन द्वारा यथानिर्धारित सक्षम प्राधिकारी [4]

4.2 प्रत्येक संगठन द्वारा की गई पहचान के अनुसार पदनामित नोडल अधिकारी [5]

4.3 भारत सरकार की ई-मेल सेवा के लिए कार्यान्वयन एजेंसी (आईए) अर्थात राष्ट्रीय सूचना विज्ञान केंद्र अथवा इस नीति के खंड 14 के अनुसार छूट प्राप्त संगठन।

5. भारत सरकार की ई-मेल सेवा की आधारभूत आवश्यकताएं

5.1 सुरक्षा

क) कार्यान्वयन एजेंसी द्वारा प्रदत्त सेवा के अलावा, ई-मेल जैसी संवेदनशील सेवा के परिनियोजन के संबंध में सुरक्षा चिंताओं को ध्यान में रखते हुए भारत सरकार के अंतर्गत कोई अन्य ई-मेल सेवा शामिल नहीं होगी।

ख) उन संगठनों, जिन्हें ''भारत सरकार की ई-मेल नीति'' के खंड 14 के अंतर्गत छूट प्रदान की गई है, को छोड़कर सभी संगठनों को अपनी ई-मेल सेवाओं को सुरक्षा कारणों से तथा नीति के एक समान प्रवर्तन हेतु कार्यान्वयन एजेंसी द्वारा परिनियोजित केंद्रीय ई-मेल सेवा में माइग्रेट करना चाहिए। निरंतरता बनाए रखने के प्रयोजन से अपनी ई-मेल सेवाओं को माइग्रेट करने वाले संगठन के ई-मेल पते माइग्रेशन प्रक्रिया के भाग के रूप में बने रहेंगे। जहां कहीं भी तकनीकी रूप से यह व्यवहार्य हो, डेटा माइग्रेशन भी किया जाएगा।

ग) भारत सरकार की ई-मेल सेवा का सुरक्षित अभिगम

i) यह सिफारिश की जाती है कि संवदेनशील कार्यालयों में कार्यरत प्रयोक्ताओं के लिए सक्षम प्राधिकारी द्वारा उचित माने गए सुरक्षित अधिप्रमाणन हेतु वर्चुअल प्राइवेट नेटवर्क (वीपीएन) [7]/वन टाइम पासवर्ड (ओटीपी) [8] का इस्तेमाल किया जाए।

ii) यह सिफारिश की जाती है कि भारत सरकार के ऐसे सरकारी अधिकारी जो लम्बी प्रतिनियुक्ति/विदेशों में कार्यरत हैं, और संवेदनशील सूचना वाले कार्य देख रहे हैं, को सक्षम प्राधिकारी उपयुक्त समझे गए अनुसार सरकारी ई-मेल सेवाओं के अभिगम के लिए वीईएन/ओटीपी का इस्तेमाल करना चाहिए।

iii) यह सिफारिश की जाती है कि विदेशों में स्थित दूतावासों और मिशनों में सक्षम प्राधिकारी द्वारा उपयुक्त समझे गए अनुसार कार्यान्वयन एजेंसी (आईए) की सेवाएं प्राप्त करने के लिए स्टेटिक आईपी एड्रेस का इस्तेमाल किया जाना चाहिए।

iv) इस संदर्भ में और अधिक सूचना "ई-मेल नीति" शीर्षक के अंतर्गत http://www.deity.gov.in/content/policiesguidelines पर उपलब्ध "ई-मेल प्रबंधन के लिए दिशानिर्देश और प्रभावी ई-मेल इस्तेमाल" में उपलब्ध हैं।

घ) सुरक्षा के परिप्रेक्ष्य में भारत सरकार की ई-मेल सेवा के सभी प्रयोक्ताओं द्वारा निम्नलिखित का अनुपालन किया जाएगा :

i) सूचना के वर्गीकरण, रखरखाव और सुरक्षा से संबंधित गृह मंत्रालय द्वारा तैयार की गईं संगत नीतियों का अनुपालन किया जाएगा।

ii) गृह मंत्रालय, भारत सरकार की संगत नीतियों के अनुसार, वगीकृत और संवेदनशील समझे जाने के कारण ई-मेल भेजने के लिए डिजिटल हस्ताक्षर प्रमाण पत्र (डीएससी) [6] के इस्तेमाल और कोडीकरण को अनिवार्य बनाया जाएगा। सुरक्षा कारणों से प्रयोक्ताओं के व्यक्तिगत प्रोफाइल के तहत चालू मोबाइल नम्बरों को अद्यतन करना अनिवार्य है। नम्बर का इस्तेमाल कार्यान्वयन एजेंसी द्वारा भेजी गई सुरक्षा से संबंधित चेतावनी और सूचना के लिए ही किया जाएगा। मोबाइल नम्बर के अलावा निजी ई-मेल आईडी (प्राथमिक रूप से भारत में मौजूदा सेवा प्रदाता से) को अद्यतन करना अनिवार्य होगा जिससे कि वैकल्पिक साधन के जरिए प्रयोक्ता को चेतावनी भेजी जा सके।

iii) प्रयोक्ता अपने सरकारी ई-मेल एकाउंट, जो भारत सरकार के ई-मेल सर्वर पर कंफिगर किया गया है, से किसी अन्य सेवा प्रदाता के पीओपी [9] अथवा आईएमएपी [10] को कंफिगर कर ई-मेल डाउनलोड नहीं करेगा। इसका निहितार्थ यह है कि प्रयोक्ताओं को अपने भारत सरकार के ई-मेल के एकाउंट के विवरण (आईडी और पासवर्ड) निजी सेवा प्रदाताओं के सर्वर पर उपलब्ध एकाउंट में नहीं देना चाहिए।

iv) किसी ऐसे प्रयोक्ता को संबोधित कोई ई-मेल, जिसका एकाउंट डिएक्टिवेट डिलीट कर दिया गया है, को अन्य ई-मेल पते पर रिडायरेक्ट नहीं किया जाएगा। ऐसे ई-मेल में हो सकता है कि कोई सरकारी सूचना सामग्री निहित हो, अत: किसी भी ई-मेल को रिडायरेक्ट नहीं किया जाएगा।

v) संगठन का संबंधित नोडल अधिकारी यह सुनिश्चित करेगा कि प्रयोक्ता के साथ समन्वय से सभी उपकरणों पर नवीनतम ऑपरेटिंग सिस्टम और एप्लीकेशन पैच उपलब्ध हों।

vi) यदि कार्यान्वयन एजेंसी के समक्ष किसी ई-मेल आईडी के साथ छेड़छाड़ का मामला आता है तो पंजीकृत मोबाइल नम्बर पर प्रयोक्ता को एक एसएमएस अलर्ट भेजा जाएगा। यदि किसी एआउंट के पासवर्ड के साथ छेड़छाड़ के "प्रयास" का मामला प्रकाश में आता है, तो एक ई-मेल अलर्ट भेजा जाएगा। ई-मेल और एसएमएस दोनों में प्रयोक्ता द्वारा की जाने वाली कार्रवाई निहित होगी। यदि प्रयोक्ता पांच बार ऐसे अलर्ट (छेड़छाड़ की जानकारी देते हुए) भेजे जाने के बावजूद भी आवश्यक कार्रवाई नहीं करता है, तो कार्यान्वयन एजेंसी के पास यह अधिकार सुरक्षित है कि वह संगत संगठन के नोडल अधिकारी सूचना देते हुए उस विशेष ई-मेल आईडी का पासवर्ड रिसेट कर सकता है।

vii) ऐसी स्थिति के मामले में जब किसी प्रयोक्ता आईडी के छेड़छाड़ का प्रभाव बड़े प्रयोक्ता आधार अथवा परिनियोजित अवसंरचना की डेटा सुरक्षा पर पड़ता है, तो कार्यान्वयन एजेंसी उस प्रयोक्ता आईडी का पासवर्ड रिसेट करेगा। यह कार्रवाई तत्काल आधार पर की जाएगी और इसकी सूचना तत्पश्चात प्रयोक्ता और नोडल अधिकारी को दी जाएगी। एसएमएस किसी प्रयोक्ता से संपर्क के प्रमुख चैनलों में से एक है; अत: सभी प्रयोक्ताओं को यह सुनिश्चित करना चाहिए कि उनके मोबाइल नम्बर अद्यतन हों।

viii) सुरक्षा कारणों से भारत सरकार द्वारा प्रदत्त ई-मेल आईडी से भारत सरकार की ई-मेल सेवा से इतर किसी अन्य सेवा प्रदाता द्वारा प्रदत्त किसी सरकारी अधिकारी के निजी अधिकारी पर ई-मेल भेजने की अनुमति नहीं। कार्यान्वयन एजेंसी द्वारा सरकारी ई-मेल आईडी का इस्तेमाल किसी अन्य प्रयोक्ता के साथ संचार हेतु इस्तेमाल किया जा सकता है चाहे वह निजी अथवा सार्वजनिक क्यों न हो। तथापि, प्रयोक्ता को ई-मेल के भाग के रूप में भेजी जा रही सूचना सामग्री पर अपने विवेकानुसार अपेक्षित सावधानी बरतनी चाहिए।

ix) सुरक्षा कारणों से सरकारी ई-मेल सेवा में पासवर्ड को ऑटोसेव करने की अनुमति नहीं होगी।

x) सुरक्षा उपायों के संबंध में अधिक विवरण "ई-मेल नीति" शीर्षक के अंतर्गत http://www.deity.gov.in/content/policiesguidelines में "एनआईसी की सुरक्षा नीति" पर उपलब्ध हैं।

xi) "ई-मेल एकाउंट प्रबंधन और प्रभावी ई-मेल इस्तेमाल के लिए दिशानिर्देश'' के अंतर्गत ई-मेल के प्रभावी इस्तेमाल के लिए दिशानिर्देश विहित किए गए हैं, जो ''ई-मेल नीति'' शीर्षक के अंतर्गत http://www.deity.gov.in/content/policiesguidelines पर उपलब्ध हैं।

5.2 ई-मेल एकाउंट प्रबंधन

क) संगत संगठनों के अनुरोध के आधार पर कार्यान्वयन एजेंसी दो आईडी बनाएगा जिनमें से एक पदनाम पर और दूसरी नाम पर आधारित होगी। जनता के साथ जिन अधिकारियों का संपर्क है उनके लिए पदनाम आधारित आईडी की सिफारिश की जाएगी। संवेदनशील प्रयोक्ताओं के लिए ई-मेल आईडी के भाग के रूप में अल्फान्यूमिरिक केरेक्टर के इस्तेमाल की सिफारिश की जाती है क्योंकि इसे सक्षम प्राधिकारी द्वारा उपयुक्त समझा गया है।

ख) सरकारी अधिकारी जो कम से कम 20 वर्ष की सेवा करने के पश्चात त्याग पत्र देते हैं अथवा अधिवर्षिता पर सेवानिवृत्त होते हैं, को पद से त्याग पत्र देने अथवा सेवानिवृत्त होने के पश्चात एक वर्ष के लिए नाम आधारित ई-मेल पता अर्थात userid@gov.in बनाए रखने की अनुमति दी जाएगी। तत्पश्चात उसी यूजर आईडी के साथ एक नया ई-मेल पता, परंतु अलग डोमेन पते (उदाहरण के लिए, userid@pension.gov.in), उनके पूरे जीवन काल के लिए कार्यान्वयन एजेंसी द्वारा उपलब्ध कराया जाएगा।

"ई-मेल एकाउंट प्रबंधन और प्रभावी ई-मेल इस्तेमाल के लिए दिशानिर्देश" के अंतर्गत ई-मेल के प्रभावी इस्तेमाल के लिए दिशानिर्देश विहित किए गए हैं, जो "ई-मेल नीति" शीर्षक के अंतर्गत http://www.deity.gov.in/content/policiesguidelines पर उपलब्ध हैं। इस दस्तावेज में ई-मेल पते बनाना, एकाउंट बनाने की प्रक्रिया, पदनाम आधारित आईडी सौंपने की प्रक्रिया, त्याग पत्र अधिवर्षिता पर सेवानिवृत्ति के पश्चात एकाउंट की स्थिति, डेटा रखना और बैकअप तथा एकाउंट डिएक्टिवेट करने जैसे विषयों को शामिल किया गया है।

5.3 पदनामित प्रशासनिक कंसोल

संगठन कार्यान्वयन एजेंसी से "पदनामित प्रशासनिक कंसोल" सेवा प्राप्त कर सकते हैं। कंसोल का इस्तेमाल करते हुए किसी संगठन का प्राधिकृत व्यक्ति संगत डोमेन के अंतर्गत आने वाली यूजर आईडी का पासवर्ड आवश्यक होने पर कार्यान्वयन एजेंसी को अनुरोध भेजे बिना बना सकता है / डिलीट/परिवर्तित कर सकता है। ऐसे संगठन जो प्रशासनिक कंसोल का चयन नहीं करते हैं, उन्हें पूर्ण विवरण के साथ अपने अनुरोध कार्यान्वयन एजेंसी के सहायता प्रकोष्ठ (support@gov.in) को भेजने होंगे।

5.4 ई-मेल डोमेन और वर्चुअल होस्टिंग

(क) भारत सरकार ई-मेल के लिए वर्चुअल डोमेन होस्टिंग की सुविधा प्रदान करती है। यदि कोई संगठन ऐसा करना चाहता है, तो कार्यान्वयन एजेंसी उनकी आवश्यकता के अनुसार उन्हें ई-मेल पतों का डोमेन प्रस्तावित कर सकती है। इसका आशय यह है कि यदि किसी संगठन को अपनी वेबसाइट, जिसका वह प्रचालन कर रहा है, से मिलता-जुलता पता आवश्यक है, तो कार्यान्वयन एजेंसी उन्हें ऐसा पता उपलब्ध करा सकती है।

(ख) प्रयोक्ताओं को बाई डिफाल्ट "userid@gov.in" सौंपा जाएगा। यूजर आईडी "ई-मेल नीति" के अंतर्गत http://www.deity.gov.in/content/policiesguidelines/ पर उपलब्ध पता निर्धारण नीति के अनुसार बनाया जाएगा।

(ग) ऐसे संगठन जो अन्य डोमेन से संबंधित कोई ई-मेल पता (अर्थात xxxx@deity.gov.in, yyyy@tourism.gov.in) प्राप्त करना चाहते हैं, तो उन्हें अपने अनुरोध कार्यान्वयन एजेंसी को भेजने होंगे।

5.5 सुरक्षित पासवर्ड का इस्तेमाल

ई-मेल सेवाओं को इस्तेमाल करने वाले सभी प्रयोक्ताओं को अपने ई-मेल एकाउंट की सुरक्षा के लिए जटिल पासवर्ड का इस्तेमाल करना चाहिए। पासवर्ड नीति के बारे में अधिक विवरण "ई-मेल नीति" शीर्षक के अंतर्गत http://www.deity.gov.in/content/policiesguidelines पर "पासवर्ड नीति" पर उपलब्ध हैं।

5.6 गोपनीयता

प्रयोक्ताओं को सुनिश्चित करना चाहिए उनके ई-मेल गोपनीय रहें। कार्यान्वयन एजेंसी गोपनीयता बनाए रखने के लिए हरसंभव सावधानी बरतेगी। प्रयोक्ताओं को यह सुनिश्चित करना चाहिए उनके पासवर्ड से संबंधित सूचना अथवा कोई अन्य निजी सूचना किसी अन्य व्यक्ति के साथ साझा न करें।

6. प्रयोक्ता संगठनों की जिम्मेदारियां

6.1 नीति का अनुपालन

(क) सभी प्रयोक्ता संगठन अपने प्रयोक्ताओं द्वारा ई-मेल नीति का अनुपालन सुनिश्चित करने के लिए उपयुक्त नियंत्रण रखेंगे। कार्यान्वयन एजेंसी इस संदर्भ में अपेक्षित सहयोग प्रदान करेगी।

(ख) कार्यान्वयन एजेंसी यह सुनिश्चित करेंगी कि उसके प्रयोक्ताओं के सरकारी ई-मेल एकाउंट केवल कार्यान्वयन एजेंसी के ई-मेल सर्वर पर ही बनाए जाएं।

(ग) कार्यान्वयन एजेंसी का नोडल अधिकारी ई-मेल नीति की सुरक्षा पहलुओं से जुड़ी सभी घटनाओं का समाधान सुनिश्चित करेगा। कार्यान्वयन एजेंसी इस संदर्भ में अपेक्षित सहयोग प्रदान करेगी।

(घ) प्रयोक्ता संगठन का सक्षम प्राधिकारी सुनिश्चित करेगा कि ई-मेल सुरक्षा पर प्रशिक्षण और जागरूकता कार्यक्रम नियमित अंतराल पर आयोजित किए जाएं। कार्यान्वयन एजेंसी इस संदर्भ में अपेक्षित सहयोग प्रदान करेगी।

6.2 नीति का प्रचार-प्रसार

(क) संबंधित संगठन के सक्षम प्राधिकारी को ई-मेल नीति का प्रचार-प्रसार सुनिश्चित करना चाहिए।

(ख) सक्षम प्राधिकारी को ई-मेल नीति पर जागरूकता पैदा करने के लिए समाचार पत्रों, बेनरों, बुलेटिन, बोर्ड आदि का इस्तेमाल करना चाहिए।

(ग) नए भर्ती किए गए अधिकारियों/कर्मचारियों के लिए अभिमुखीकरण कार्यक्रम में ई-मेल नीति पर एक सत्र शामिल किया जाना चाहिए।

7. प्रयोक्ताओं की जिम्मेदारियां

7.1 ई-मेल सेवाओं का उपयुक्त इस्तेमाल

(क) ई-मेल की सुविधा प्रयोक्ताओं को अपनी सरकारी जिम्मेदारियों को पूरा करने में सहायता के लिए एक व्यावसायिक संसाधन के रूप में उपलब्ध कराई जाती है। सरकारी पत्राचार के लिए पदनाम आधारित आईडी का इस्तेमाल किया जाना चाहिए और नाम आधारित आईडी का इस्तेमाल सरकारी और निजी दोनों प्रकार के पत्राचार के लिए किया जा सकता है।

(ख) **ई-मेल सेवाओं के गलत इस्तेमाल के उदाहरण**

i) ऐसे ई-मेल बनाना और उनका लेन-देन करना जिन्हें अपमानजनक, अश्लील अथवा धमकी देने वाली ई-मेल श्रेणी में रखा जा सकता है।

ii) किसी के स्वामित्व वाली सूचना अथवा अन्य कोई सुविधायुक्त, गोपनीय या संवेदनशील सूचना का अनाधिकृत लेन-देन।

iii) सेवाओं का अनाधिकृत अभिगम। इसमें बेनामी ई-मेल भेजना, किसी अन्य अधिकारी के यूजर आईडी का इस्तेमाल अथवा किसी छद्म पहचान का इस्तेमाल शामिल है।

iv) ज्ञापन, प्रलोभन, श्रृंखला पत्र और अन्य गैर-सरकारी, धमकी भरे ई- मेल बनाना और लेन-देन करना।

v) कॉपीराइट कानून सहित किसी विधि के उल्लंघन में सूचना बनाना और लेन-देन करना।

vi) किसी कम्प्यूटर वायरस वाले ई-मेल को जानबूझ कर भेजना।

vii) किसी ई-मेल के भेजने वाले की पहचान की गलत प्रतिनिधित्व करना।

viii) किसी अन्य व्यक्ति के एकाउंट का उसकी अनुमति के बिना इस्तेमाल करना अथवा इस्तेमाल के लिए प्रयास करना।

ix) ऐसे ई-मेल भेजना जिनमें धर्म, जाति, नीतिवाद के विरुद्ध अभद्र भाषा का इस्तेमाल, किसी प्रसारण सूची को निजी ई-मेल भेजना, ऐसे ई-मेल का लेन-देन जिसमें राष्ट्रविरोधी संदेश निहित हो, अश्लील सामग्रीयुक्त ई-मेल भेजना आदि शामिल हैं।

x) ई-मेल, जो निजी प्रकृति की हैं जैसे निजी कार्य आदि, भेजने के प्रयोजन से वितरण सूचियों का इस्तेमाल।

ई-मेल एकाउंट के गलत इस्तेमाल के किसी भी मामले को इस नीति का उल्लंघन माना जाएगा और इसके परिणामस्वरूप एकाउंट डिएक्टिवेट [11] किया जा सकता है। इसके अलावा, ऐसी घटनाओं की जांचकर्ता एजेंसियों द्वारा उल्लंघन की प्रकृति के आधार पर जांच भी की जा सकती है।

7.2 प्रयोक्ता की भूमिका

(क) सरकारी ई-मेल प्रणाली का इस्तेमाल करते हुए भेजे गए किसी डेटा/ ई-मेल के लिए प्रयोक्ता जिम्मेदार है। ई-मेल सर्वर के जरिए भेजे गए सभी ई-मेल/डेटा के लिए वही प्रयोक्ता पूरी तरह से जिम्मेदार है जिसका एकाउंट इस्तेमाल किया जाता है।

(ख) पासवर्ड साझा करना प्रतिबंधित है।

(ग) प्रयोक्ता निम्नलिखित के लिए भी जिम्मेदार होगा :

(i) प्रयोक्ता उन्हें दिए गए एकाउंट का इस्तेमाल करते हुए उनकी ग्राहक प्रणालियों में किए गए कार्यकलापों के लिए जिम्मेदार होंगे।

(ii) 'रिप्लाई ऑल' और 'वितरण सूचियों' जैसे विकल्पों का इस्तेमाल सावधानीपूर्वक किया जाना चाहिए ताकि गलत लोगों को ई-मेल भेजने का जोखिम कम किया जा सके।

(iii) प्रयोक्ता द्वारा महत्वपूर्ण फाइलों का बेक-अप नियमित अंतराल पर लिया जाएगा । कार्यान्वयन एजेंसी प्रयोक्ता की कार्रवाई के कारण होने वाली डेटा हानि को रिस्टोर नहीं करेगी ।

8. सेवा स्तर करार

कार्यान्वयन एजेंसी "ई-मेल नीति" के अंतर्गत http://www.deity.gov.in/content/policiesguidelines पर सेवा स्तर करार (एसएलए) के आधार पर ई-मेल सेवाएं उपलब्ध कराएगी ।

9. ई-मेल की जांच/लॉग जारी करना

9.1 उपर्युक्त खंडों में किसी भी बात के होते हुए भी कार्यान्वयन एजेंसी द्वारा कानून प्रवर्तन एजेंसियों और अन्य संगठनों को लॉग/ई-मेल का प्रकटन सूचना प्रौद्योगिकी अधिनियम 2000 और अन्य लागू विधियों के अनुसार ही किया जाएगा ।

9.2 कार्यान्वयन एजेंसी किसी संगठन से अनुरोध प्राप्त होने तक ई-मेल की जांच अथवा लॉग जारी करने के लिए तब तक कोई कार्रवाई नहीं करेगी और न ही अनुरोध स्वीकार करेगी जब कि इस खंड में ऐसा प्रावधान न किया गया हो ।

9.3 कार्यान्वयन एजेंसी दो वर्ष की अवधि के लिए लॉग बनाए रखेगी ।

10. सुरक्षा घटना प्रबंधन प्रक्रिया

10.1 किसी सुरक्षा घटना को ऐसी प्रतिकूल घटना के रूप में परिभाषित किया जाता है जो सरकारी डेटा की उपलब्धता, सत्यनिष्ठा, गोपनीयता और प्राधिकार को प्रभावित कर सकती है । सुरक्षा घटनाएं मालवेयर, फिशिंग, [12] उपकरण की क्षति, किसी ई-मेल आईडी के साथ छेड़छाड़ आदि के कारण घटित हो सकती है ।

10.2 यदि यह पाया जाता है कि कोई ई-मेल सेवा से खतरा उत्पन्न हो सकता है और इसके चलते छेड़छाड़ की घटना हो सकती है तो कार्यान्वयन एजेंसी इसकी किसी विशेषता को डिएक्टिवेट अथवा हटा सकती है ।

10.3 प्रयोक्ता द्वारा पायी गई अथवा पहचान की गई किसी सुरक्षा घटना की सूचना तत्काल भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) और कार्यान्वयन एजेंसी को तत्काल दी जानी चाहिए ।

11. बौद्धिक संपदा

11.1 कार्यान्वयन एजेंसी की ई-मेल सेवा और संसाधनों के जरिए अभिगमयोग्य सामग्री गोपनीयता, प्रचार-प्रसार अथवा अन्य व्यक्तिगत अधिकारों और बौद्धिक संपदा अधिकारों के अंतर्गत सुरक्षा के अध्यधीन हो, जिसमें कॉपीराइट और पेटेंट, ट्रेडमार्क, ट्रेड सीक्रेट अथवा अन्य मालिकाना सूचना, परंतु इतना ही नहीं शामिल होंगे । प्रयोक्ता ऐसे किसी भी ढंग से सरकारी सेवा और संसाधनों का इस्तेमाल नहीं करेंगे जो ऐसे किसी अधिकार का उल्लंघन, गलत व्याख्या करती हो अथवा अन्यथा उसका उल्लंघन करती हो ।

12. प्रवर्तन

12.1 यह "ई-मेल नीति" खंड 2.2 में यथाविनिर्दिष्ट सभी सरकारी कर्मचारियों के लिए लागू है ।

12.2 प्रत्येक संगठन इस नीति के प्रावधानों का अनुपालन सुनिश्चित करने के लिए जिम्मेदार होगा । कार्यान्वयन एजेंसी इस संदर्भ में संगठनों को आवश्यक तकनीकी सहायता प्रदान करेगी ।

13. डिएक्टिवेशन

13.1 सरकारी सेवा की सुरक्षा के लिए खतरे के मामले में प्रयुक्त ई-मेल आईडी, जो सेवा को प्रभावित कर सकता है, को कार्यान्वयन एजेंसी द्वारा तत्काल बंद अथवा डिएक्टिवेट किया जाए ।

13.2 डिएक्टिवेशन के पश्चात संबंधित प्रयोक्ता और संगत संगठन के समक्ष प्राधिकारी को सूचना दी जाएगी ।

14. छूट

14.1 ऐसे संगठन, जिनमें राष्ट्रीय सुरक्षा से जुड़े संगठन शामिल हैं, जिनके पास वर्तमान में अपने स्वतंत्र मेल सर्वर उपलब्ध हैं, वे इनका प्रचालन जारी रख सकते हैं, बशर्ते कि उनके ई-मेल सर्वर भारत में स्थापित हों । तथापि, इन संगठनों को यह सुनिश्चित करना आवश्यक है कि ई-मेल नीति के सिद्धांतों का अनुपालन किया जाए । परंतु, समान रूप से नीति के प्रवर्तन और सुरक्षा के हित में यह सिफारिश की जाती है कि इन संगठनों को भी कार्यान्वियन एजेंसी की प्रमुख सेवा को अपनाने के लिए विचार करना चाहिए ।

14.2 विदेश में स्थित भारतीय मिशन में पदस्थ सरकारी अधिकारी आकस्मिक परिस्थितियों जैसे इंटरनेट सेवाओं के बाधित होने, जिसके चलते सरकारी ई-मेल सेवाएं उपलब्ध नहीं होंगी, में स्थानीय संचार चैनलों की उपलब्धता सुनिश्चित करने के लिए भारत से बाहर होस्ट की गई वैकल्पिक ई-मेल सेवाओं को बनाए रख सकते हैं ।

14.3 एयर गेप के साथ इंट्रानेट[13] मेल सर्वरों का प्रचालन करने वाले संगठनों को इस नीति से छूट प्रदान की जाती है ।

15. ई-मेल सेवाओं की जांच (ऑडिट)

एनआईसी की ई-मेल सेवाओं और अन्य संगठन जिनके अपने स्वयं के मेल सर्वर हैं, की सुरक्षा जांच डीआईटी द्वारा अनुमोदित संगठन के माध्यम से आवधिक रूप से की जाएगी ।

16. समीक्षा

अंतर-मंत्रालयी परामर्श के उपरांत संचार और सूचना प्रौद्योगिकी मंत्री के अनुमोदन से आवश्यक होने पर नीतियों में आगे परिवर्तन किए जाएंगे ।

आर. एस. शर्मा, सचिव

शब्दावली

क्र.सं.	शब्द	परिभाषा
1	**प्रयोक्ता**	प्र ोक्ता से ऐसे सरकारी/राज /संघ राज सरकार के कर्मचारि ों से अभिप्रेत है जो सरकारी ई-मेल सेवाओं का अभिगम करते हैं ।
2	**कार्यान्वयन एजेंसी (आईए)**	इस नीति के प्र ोजन से का न्वि न एजेंसी इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग, संचार और सूचना प्रौद्योगिकी मंत्राल , भारत सरकार के अधीन "राष्ट्री सूचना विज्ञान केंद्र" अभिप्रेत है ।
3	**संगठन**	इस नीति के प्र ोजन से संगठन से केंद्र और राज दोनों स्तरों पर सभी मंत्राल ों/विभागों/का लि ों/सांविधिक निका ों/ स्वा त्त निका ों से अभिप्रेत है । ऐसे सरकारी संगठन इसमें शामिल नहीं हैं जो वाणिजि क सेवाएं प्रदान करते हैं ।
4	**सक्षम प्राधिकारी**	सक्षम प्राधिकारी से अपने संगठन में इस नीति से संबंधित सभी निर्ण लेने और अनुमोदन करने के लिए जिम्मेदार अधिकारी अभिप्रेत है ।
5.	**नोडल अधिकारी**	नोडल अधिकारी से ऐसा अधिकारी अभिप्रेत है जो इस नीति के संबंध में सभी मामलों के लिए जवाबदेह है और जो संगठन की ओर से इस संबंध में समन्वय करेगा ।
6	**डीएससी**	**डिजिटल हस्ताक्षर** किसी डिजिटल संदेश अथवा दस्तावेज की प्रमाणिकता प्रदर्शित करने के लिए एक गणिती ोजना है । वैध डिजिटल हस्ताक्षर वाले ई-मेल से प्राप्तकर्ता को ह विश्वास होता है कि ई-मेल किसी जानकार ् क्ति ने भेजी है, इस प्रकार, भेजने वाला ई-मेल भेजने की बात को स्वीकार करने से मना (अधिप्रमाणन और खंडन न करना) नहीं कर सकता और ह बात भी सिद्ध हो जाती है कि पारगमन (सत निष्ठा) के समय ई-मेल में कोई परिवर्तन नहीं कि ा ग ा है ।
7	**वीपीएन**	**वर्चुअल प्राइवेट नेटवर्क** इंटरनेट जैसे किसी सार्वजनिक नेटवर्क के परे एक निजी नेटवर्क का विस्तार करता है । ह किसी कम्प् ूटर को साझा अथवा सार्वजनिक नेटवर्क से परे डेटा भेजने और प्राप्त करने में उसी प्रकार समर्थ बनाता है जैसे मानो ह सीधे उसी निजी नेटवर्क से जुड़ा हो, इससे जहां एक ओर, प्रका त्मिकता का लाभ प्राप्त होता है, वहीं दूसरी निजी नेटवर्क की सुरक्षा और प्रबंधन नीति ों का भी अनुपालन सुनिश्चित होता है ।

8	**ओटीपी**	**वन टाइम पासवर्ड (ओटीपी)** एक ऐसा पासवर्ड है जो केवल एक बार लॉगिन सत्र अथवा लेन-देन के लिए ही वैध होता है। ओटीपी ऐसी बहुत सी कमि ों से बचाता है जो पारंपरिक (स्थाई) पासवर्डों से जुड़ी होती हैं।
9	**पीओपी**	**पीओपी** एक प्रकार का पोस्ट ऑफिस प्रोटोकॉल है, जिसका इस्तेमाल किसी मेल सर्वर से ई-मेल का पता लगाने के लिए कि ा जाता है।
10	**आईएमएपी**	**आईएमएपी** एक प्रकार का **"द इंटरनेट मैसेज एक्सेस प्रोटोकॉल"** है, जिसका इस्तेमाल किसी दूरस्थ मेल सर्वर से ई-मेल का पता लगाने के लिए कि ा जाता है। पीओपी के विपरीत आईएमएपी में संदेश आपके स्थानी कम्प ूटर पर प्रदर्शित किए जाते हैं, परंतु उन्हें मेल सर्वर पर रखा और भंडारित कि ा जाता है। आईएमएपी आपको ई-मेल सर्वर पर अपने फोल्डर सिंक करने की अनुमति प्रदान करता है, जो पीओपी का इस्तेमाल करने पर संभव नहीं है।
11	**डिएक्टिवेशन**	किसी एकाउंट के **डिएक्टिवेशन** से अभिप्रेत है कि एकाउंट का अभिगम आगे नहीं कि ा जा सकेगा। डिएक्टिवेट किए गए एकाउंट में भेजे गए सभी ई-मेल भेजने वाले को बाउंस कर दिए जाएंगे।
12	**फिशिंग**	**फिशिंग** धोखाधड़ी का एक प्र ास है, जो सामान् त: ई-मेल के जरिए किसी प्र ोक्ता की निजी सूचना चोरी करने के लिए कि ा जाता है। फिशिंग ई-मेल में किसी प्र ोक्ता को लगभग हमेशा ऐसे लिंक पर क्लिक करने के लिए अनुरोध कि ा जाता है जो प्र ोक्ता को एक अलग साइट पर ले जाता है जहां उससे निजी सूचना देने का अनुरोध कि ा जाता है। वैध संगठन ई-मेल द्वारा ऐसी सूचना के लिए कभी अनुरोध नहीं करेंगे। प्र ोक्ताओं को ऐसे किसी लिंक पर कभी क्लिक नहीं करना चाहिए। किसी भी प्र ोक्ता को कोई भी ूआरएल हमेशा ब्राउज़र में ही टाइप करना चाहिए भले ही लिंक सही प्रतीत क ों न हो रही हो।
13	**इंट्रानेट**	इंट्रानेट एक निजी नेटवर्क होता है जो किसी संगठन के भीतर निहित होता है। इस नीति के प्र ोजन से किसी इंट्रानेट से जुड़े कम्प ूटरों को इंटरनेट से जोड़ने की अनुमति नहीं होती है।

MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY
(Department of Electronics and Information Technology)

NOTIFICATION

New Delhi, the 18th February, 2015

Subject: E-mail policy of Government of India

F. No. 2(22)/2013-EG-II.—1. Introduction

1.1 The Government uses e-mail as a major mode of communication. Communications include Government of India (GoI) data that travel as part of mail transactions between users [1] located both within the country and outside.

1.2 This policy of Government of India lays down the guidelines with respect to use of e-mail services. The Implementing Agency (IA) [2] for the GoI e-mail service shall be National Informatics Centre (NIC), under the Department of Electronics and Information Technology (DeitY), Ministry of Communications and Information Technology. The organisations exempted under Clause 14 will themselves become the Implementing Agency (IA) for the purpose of this policy.

2. Scope

2.1 Only the e-mail services provided by NIC, the Implementing Agency of the Government of India shall be used for official communications by all organizations except those exempted under clause no 14 of this policy. The e-mail services provided by other service providers shall not be used for any official communication.

2.2 This policy is applicable to all employees of GoI and employees of those State/UT Governments that use the e-mail services of GoI and also those State/UT Governments that choose to adopt this policy in future. The directives contained in this policy must be followed by all of them with no exceptions. All users of e-mail services can find further information in the supporting policies available on http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

2.3 E-mail can be used as part of the electronic file processing in Government of India. Further information in this regard is available at: http://darpg.gov.in/darpgwebsite_cms/Document/file/CSMeOP_1st_Edition.pdf.

3. Objective

3.1 The objective of this policy is to ensure secure access and usage of Government of India e-mail services by its users. Users have the responsibility to use this resource in an efficient, effective, lawful, and ethical manner. Use of the Government of India e-mail service amounts to the user's agreement to be governed by this policy.

3.2 All services under e-mail are offered free of cost to all officials under Ministries / Departments / Statutory Bodies / Autonomous bodies (henceforth referred to as "Organization [3]" in the policy) of both Central and State/UT Governments. More information is available under "NIC e-mail Services and Usage Policy" at http://www.deity.gov.in/content/policiesguidelines/ under the caption "E-mail Policy".

3.3 Any other policies, guidelines or instructions on e-mail previously issued shall be superseded by this policy.

4. Roles specified for implementation of the Policy

The following roles are specified in each organization using the GoI e-mail service. The official identified for the task shall be responsible for the management of the entire user base configured under that respective domain.

4.1 Competent Authority[4] as identified by each organization

4.2 Designated nodal officer[5] as identified by each organization

4.3 GoI e-mail service Implementing Agency (IA), i.e. National Informatics Centre or the exempt organisation as per Clause 14 of this policy.

5. Basic requirements of GoI e-mail Service

5.1 Security

a) Considering the security concerns with regard to a sensitive deployment like e-mail, apart from the service provided by the IA, there would not be any other e-mail service under GoI.

b) All organizations, except those exempted under clause 14 of this policy, should migrate their e-mail services to the centralized deployment of the IA for security reasons and uniform policy enforcement. For the purpose of continuity, the e-mail address of the organization migrating their service to the IA deployment shall be retained as part of the migration process. Wherever it is technically feasible, data migration shall also be done.

c) Secure access to the GoI email service

i) It is recommended for users working in sensitive offices to use VPN[7]/OTP[8] for secure authentication as deemed appropriate by the competent authority.

ii) It is recommended that GoI officials on long deputation/stationed abroad and handling sensitive information should use (VPN)/ (OTP) for accessing GoI e-mail services as deemed appropriate by the competent authority.

iii) It is recommended that Embassies and missions abroad should use Static IP addresses for accessing the services of the IA as deemed appropriate by the competent authority.

iv) More information is available under "Guidelines for E-mail Management and Effective E-mail Usage" at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

d) From the perspective of security, the following shall be adhered to by all users of GoI e-mail service:

i) Relevant Policies framed by Ministry of Home Affairs, relating to classification, handling and security of information shall be followed.

ii) Use of Digital Signature Certificate (DSC) [6] and encryption shall, be mandatory for sending e-mails deemed as classified and sensitive, in accordance with the relevant policies of Ministry of Home Affairs. Updation of current mobile numbers under the personal profile of users is mandatory for security reasons. The number would be used only for alerts and information regarding security sent by the IA. Updation of personal e-mail id (preferably from a service provider within India), in addition to the mobile number, shall also be mandatory in order to reach the user through an alternate means for sending alerts.

iii) Users shall not download e-mails from their official e-mail account, configured on the GoI mail server, by configuring POP [9] or IMAP [10] on any other e-mail service provider. This implies that users should not provide their GoI e-mail account details (id and password) to their accounts on private e-mail service providers.

iv) Any e-mail addressed to a user, whose account has been deactivated /deleted, shall not be redirected to another e-mail address. Such e-mails may contain contents that belong to the Government and hence no e-mails shall be redirected.

v) The concerned nodal officer of the organization shall ensure that the latest operating system, anti-virus and application patches are available on all the devices, in coordination with the User.

vi) In case a compromise of an e-mail id is detected by the IA, an SMS alert shall be sent to the user on the registered mobile number. In case an "attempt" to compromise the password of an account is detected, an e-mail alert shall be sent. Both the e-mail and the SMS shall contain details of the action to be taken by the user. In case a user does not take the required action even after five such alerts (indicating a compromise), the IA reserves the right to reset the password of that particular e-mail id under intimation to the nodal officer of that respective organization.

vii) In case of a situation when a compromise of a user id impacts a large user base or the data security of the deployment, the IA shall reset the password of that user id. This action shall be taken on an immediate basis, and the information shall be provided to the user and the nodal officer subsequently. SMS shall be one of the prime channels to contact a user; hence all users should ensure that their mobile numbers are updated.

viii) Forwarding of e-mail from the e-mail id provided by GoI to the Government official's personal id outside the GoI e-mail service is not allowed due to security reasons. Official e-mail id provided by the IA can be used to communicate with any other user, whether private or public. However, the user must exercise due discretion on the contents that are being sent as part of the e-mail.

ix) Auto-save of password in the Government e-mail service shall not be permitted due to security reasons.

x) More details regarding security measures are available in "NIC Security Policy" at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

xi) The guidelines for effective e-mail usage have been described in "Guidelines for E-mail Account Management and Effective E-mail Usage" available at http://www.deity.gov.in/content/policiesguidelines under the caption "Email Policy".

5.2 E-mail Account Management

a) Based on the request of the respective organizations, IA will create two ids, one based on the designation and the other based on the name. Designation based id's are recommended

for officers dealing with the public. Use of alphanumeric characters as part of the e-mail id is recommended for sensitive users as deemed appropriate by the competent authority.

b) Government officers who resign or superannuate after rendering at least 20 years of service shall be allowed to retain the name based e-mail address i.e. userid@gov.in for one year post resignation or superannuation. Subsequently, a new e-mail address with the same user id but with a different domain address (for instance, userid@pension.gov.in), would be provided by the IA for their entire life.

More details pertaining to e-mail account management are provided in "Guidelines for E-mail Account Management and Effective E-mail Usage"" available at http://www.deity.gov.in/content/policiesguidelines under the caption "Email Policy". The document covers creation of E-mail addresses, process of account creation, process of handover of designation-based ids, status of account after resignation and superannuation, data retention & backup and deactivation of accounts.

5.3 Delegated Admin Console

Organizations can avail the "Delegated Admin Console" service from IA. Using the console the authorized person of an organization can create/delete/change the password of user ids under that respective domain as and when required without routing the request through IA. Organizations that do not opt for the admin console need to forward their requests with complete details to the IA's support cell (support@gov.in).

5.4 E-mail Domain & Virtual Hosting

a) GoI provides virtual domain hosting for e-mail. If an organization so desires, the IA can offer a domain of e-mail addresses as required by them. This implies that if an organization requires an address resembling the website that they are operating, IA can provide the same.

b) By default, the address "userid@gov.in" shall be assigned to the users. The user id shall be created as per the addressing policy available at http://www.deity.gov.in/content/policiesguidelines/ under "E-mail Policy".

c) Organizations desirous of an e-mail address belonging to other domains (e.g. xxxx@deity.gov.in, yyyy@tourism.gov.in) need to forward their requests to the IA

5.5 Use of Secure Passwords

All users accessing the e-mail services must use strong passwords for security of their e-mail accounts. More details about the password policy are available in "Password Policy" at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

5.6 Privacy

Users should ensure that e-mails are kept confidential. IA shall take all possible precautions on maintaining privacy. Users must ensure that information regarding their password or any other personal information is not shared with anyone.

6. Responsibilities of User Organizations

6.1 Policy Compliance

a) All user organizations shall implement appropriate controls to ensure compliance with the e-mail policy by their users. IA shall give the requisite support in this regard.

b) The user organizations shall ensure that official e-mail accounts of all its users are created only on the e-mail server of the IA.

c) Nodal officer of the user organization shall ensure resolution of all incidents related to the security aspects of the e-mail policy. IA shall give the requisite support in this regard.

d) Competent Authority of the user organization shall ensure that training and awareness programs on e-mail security are organized at regular intervals. Implementing Agency shall provide the required support.

6.2 Policy Dissemination

a) Competent Authority of the concerned organization should ensure dissemination of the e-mail policy.

b) Competent Authority should use Newsletters, banners, bulletin boards etc, to facilitate increased awareness on the e-mail policy.

c) Orientation programs for new recruits shall include a session on the e-mail policy.

7. Responsibilities of Users

7.1 Appropriate Use of E-mail Service

a) E-mail is provided as a professional resource to assist users in fulfilling their official duties. Designation based ids should be used for official communication and name based ids can be used for both official and personal communication.

b) Examples of inappropriate use of the e-mail service

i) Creation and exchange of e-mails that could be categorized as harassing, obscene or threatening.

ii) Unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

iii) Unauthorized access of the services. This includes the distribution of e-mails anonymously, use of other officers' user ids or using a false identity.

iv) Creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.

v) Creation and exchange of information in violation of any laws, including copyright laws.

vi) Wilful transmission of an e-mail containing a computer virus.

vii) Misrepresentation of the identity of the sender of an e-mail.

viii) Use or attempt to use the accounts of others without their permission.

ix) Transmission of e-mails involving language derogatory to religion, caste, ethnicity, sending personal e-mails to a broadcast list, exchange of e-mails containing anti-national messages, sending e-mails with obscene material, etc.

x) Use of distribution lists for the purpose of sending e-mails that are personal in nature, such as personal functions, etc.

Any case of inappropriate use of e-mail accounts shall be considered a violation of the policy and may result in deactivation [11] of the account. Further, such instances may also invite scrutiny by the investigating agencies depending on the nature of violation.

7.2 User's Role

a) The User is responsible for any data/e-mail that is transmitted using the GoI e-mail system. All e-mails/data sent through the mail server are the sole responsibility of the user owning the account.

b) Sharing of passwords is prohibited.

c) The user's responsibility shall extend to the following:

i) Users shall be responsible for the activities carried out on their client systems, using the accounts assigned to them.

ii) The 'reply all' and the use of 'distribution lists' should be used with caution to reduce the risk of sending e-mails to wrong people.

iii) Back up of important files shall be taken by the user at regular intervals. The IA shall not restore the data lost due to user's actions.

8. Service Level Agreement

The IA shall provide the e-mail services based on the Service Level Agreement (SLA) available at http://www.deity.gov.in/content/policiesguidelines under the caption "E-mail Policy".

9. Scrutiny of e-mails/Release of logs

9.1 Notwithstanding anything in the clauses above, the disclosure of logs/e-mails to law enforcement agencies and other organizations by the IA would be done only as per the IT Act 2000 and other applicable laws.

9.2 The IA shall neither accept nor act on the request from any other organization, save as provided in this clause, for scrutiny of e-mails or release of logs.

9.3 IA will maintain logs for a period of two years.

10. Security Incident Management Process

10.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Government data. Security incidents can be due to factors like malware, phishing [12], loss of a device, compromise of an e-mail id etc.

10.2 It shall be within the right of the IA to deactivate or remove any feature of the e-mail service if it is deemed as a threat and can lead to a compromise of the service.

10.3 Any security incident, noticed or identified by a user must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.

11. Intellectual Property

11.1 Material accessible through the IA's e-mail service and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Government service and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

12. Enforcement

12.1 This "E-mail policy" is applicable to all Government employees as specified in clause 2.2.

12.2 Each organization shall be responsible for ensuring compliance with the provisions of this policy. The Implementing Agency would provide necessary technical assistance to the organizations in this regard.

13. Deactivation

13.1 In case of threat to the security of the Government service, the e-mail id being used to impact the service may be suspended or deactivated immediately by the IA.

13.2 Subsequent to deactivation, the concerned user and the competent authority of that respective organization shall be informed.

14. Exemption

14.1 Organizations, including those dealing with national security, that currently have their own independent mail servers can continue to operate the same, provided the e-mail servers are hosted in India. These organizations however need to ensure that the principles of the e-mail

policy are followed. However, in the interest of uniform policy enforcement and security, it is recommended that these organizations should consider migrating to the core service of the IA.

14.2 Indian Missions and Posts abroad may, however, maintain alternative e-mail services hosted outside India to ensure availability of local communication channels under exigent circumstances such as disruption of internet services that can cause non-availability of Government e-mail services.

14.3 Organizations operating Intranet [13] mail servers with air-gap are exempted from this policy.

15. Audit of E-mail Services

The security audit of NIC email services and other organizations maintaining their own mail server shall be conducted periodically by an organization approved by Deity.

16. Review

Future changes in this Policy, as deemed necessary, shall be made by DeitY with approval of the Minister of Communication & IT after due inter-ministerial consultations.

R. S. SHARMA, Secy.

GLOSSARY

S.No	TERM	DEFINITION
1	**Users**	Refers to Government/State/UT employees who are accessing the Government e-mail services.
2	**Implementing agency (IA)**	For the purpose of this policy, the implementing agency is "National Informatics Centre" under the Department of Electronics and Information Technology, Ministry of Communications and Information Technology, Government of India
3	**Organization**	For the purpose of this policy, organisation refers to all ministries/departments/ offices/statutory bodies/autonomous bodies, both at the Central and State level. Government organizations offering commercial services are not included.
4	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his Organization
5.	**Nodal Officer**	Officer responsible for all matters relating to this policy who will coordinate on behalf of the Organization
6	**DSC**	A **digital signature** is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives the recipient reason to believe that the e-mail was created by a known sender, such that the sender cannot deny having sent the e-mail (authentication and non-repudiation) and that the e-mail was not altered in transit (integrity).
7	**VPN**	A **virtual private network** extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network
8	**OTP**	A **one-time password** (OTP) is a password that is valid for only one login session or transaction. OTPs avoid a number of shortcomings that are associated with traditional (static) passwords
9	**POP**	**POP is** short for **P***ost* **O***ffice* **P***rotocol,* a protocol used to retrieve e-mail from a mail server.

10	**IMAP**	IMAP is short for **"The Internet Message Access Protocol",** a protocol used to retrieve e-mail from a remote mail server. Unlike POP, in IMAP, Messages are displayed on your local computer but are kept and stored on the mail server. IMAP allows you to sync your folders with the e-mail server which is not possible using POP.
11	**Deactivation**	**Deactivation** of an account means that the account can no longer be accessed. All e-mails sent to a deactivated account shall bounce to the sender
12	**Phishing**	**Phishing** is a fraudulent attempt, usually made through e-mail, to steal a user's personal information. Phishing e-mails almost always tell a user to click a link that takes the user to a site from where the personal information is requested. Legitimate organisations would never request this information via e-mail. Users should never click on a link. A user should always type a URL in the browser even if the link appears genuine**.**
13	**Intranet**	An intranet is a private network that is contained within an organization. For the purpose of this policy, computers connected to an intranet are not allowed to connect to internet.

Printed by the Manager, Government of India Press, Ring Road, Mayapuri, New Delhi-110064
and Published by the Controller of Publications, Delhi-110054.