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. 45] नई दिल्ली, बृहस्पतिवार, फरवरी 19, 2015/माघ 30, 1936
No. 45] NEW DELHI, THURSDAY, FEBRUARY 19, 2015/MAGHA 30, 1936

संचार और सूचना प्रौद्योगिकी मंत्रालय
(इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग)
अधिसूचना

नई दिल्ली 18 फ़रवरी, 2015

विषय : भारत सरकार के आईटी संसाधनों के इस्तेमाल पर नीति।

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

1.1. सरकार अपने कर्मचारियों की क्षमता और उत्पादकता को बढ़ाने के लिए आईटी संसाधन उपलब्ध कराती है। ये संसाधन अपने कार्य क्षेत्र से संबंधी सूचना तक पहुंच बनाने और उसे तैयार करने के टूल के रूप में है। ये संसाधन सरकारी कर्मचारियों तक समय से सूचना पहुंचाने और सक्षम और प्रभावी ढंग से कार्य करने में मदद करते हैं।

1.2. इस नीति के उद्देश्य से, 'आईटी संसाधन' शब्द से वायरलैस नेटवर्क, इंटरनेट कनेक्टिविटी, एक्सटर्नल स्टोरेज डिवाइसें और प्रिंटर और स्कैनर जैसे बाह्य उपकरण और उनसे जुड़े सॉफ्ट्वेयर समेत डेस्कटॉप उपकरण, पोर्टेबल और मोबाइल उपकरण, नेटवर्क शामिल हैं।

1.3. सरकार के लिए संसाधनों का दुरपयोग से सरकार के लिए अवांछनीय खतरे और दायित्व पैदा हो सकते हैं। अत: उम्मीद यह की जाती है कि इन संसाधनों का उपयोग प्राथमिक रूप से सरकार संबंधी उद्देश्यों के कानूनी और नीतिपरक रूप से किया जाए।

2. कार्यक्षेत्र

यह नीति अंतिम प्रयोग [1] की दृष्टि से आईटी संसाधनों के प्रयोग को निर्धारित करती हैं। यह नीति भारत सरकार के सभी कर्मचारियों पर लागू होती है और उन राज्य/संघ राज्य क्षेत्र की सरकारों के कर्मचारियों पर लागू होती है, जो भारत सरकार के आईटी संसाधनों का प्रयोग करते हैं और उन राज्य/संघ राज्य क्षेत्र की सरकारों पर भी जो भविष्य में इस नीति को अपनाने का विकल्प चुनते हैं।

3. उद्देश्य

इस नीति का उद्देश्य सरकार के आईटी संसाधनों तक समुचित पहुंच और प्रयोग सुनिश्चित करना है और प्रयोक्ताओं के द्वारा उनका दुरूपयोग रोकता है । भारत सरकार द्वारा उपलब्ध कराए गए संसाधनों के उपयोग का अर्थ है कि प्रयोक्ता के साथ किए गए करार का नियंत्रण इस नीति द्वारा किया जाएगा ।

4. भूमिकाएं और जिम्मेदारियां

केन्द्र/राज्य/संघ क्षेत्र सरकार के आईटी संसाधनों के इस्तेमाल द्वारा प्रत्यक संगठन [2] में निम्नलिखित भूमिकाओं की आवश्यकता है । इस कार्य के लिए चिन्हित कर्मचारी अपनी संबंधित डोमेन के अंतर्गत समग्र यूजर बेस के इस्तेमाल के लिए नियोजित आईटी संसाधनों के प्रबंधन के लिए जिम्मेदार होगा ।

4.1 प्रत्येक संगठन द्वारा यथा चिन्हित सक्षम प्राधिकारी [3] ।

4.2 प्रत्येक संगठन द्वारा यथा चिन्हित नामित नोडल अधिकारी [4]।

4.3 कार्यान्वयन एजेंसी [5]: सूचना सुरक्षा की समग्री जिम्मेदारी संबंधित संगठन की होगी । नेटवर्क सेवाओं की सुरक्षा के हित में यह सिफारिश की गई है कि संगठनों को एनआईसी द्वारा उपलब्ध कराई गई भारत सरकार की नेटवर्क सेवाओं का इस्तेमाल करना चाहिए, जिसके मामले में सबंधित सगंठन की तरफ से नेटवर्क सेंवाओं की सुरक्षा हेतु, एनआईसी कार्यान्वयन एजेंसी होगी ।

4.4 नेटवर्क सेवाओं को छोड़कर सभी आईटी संसाधनों का प्रबंध करने के लिए संबंधित संगठन, नोडल एजेंसी होगा [6]।

5. नेटवर्क तक पहुंच

5.1. *इंटरनेट और इंट्रॉनेट तक पहुंच*

क) प्रयोक्ता क्लाइंट सिस्टम को सरकारी नेटवर्क से जोड़ने से पहले सक्षम प्राधिकारी से एक बार में अनुमोदन प्राप्त करेगा और क्लाइंट सिस्टम को रजिस्टर करेगा ।

ख) इस बात की पुरजोर सिफारिश की जातीहै कि संवेदनशील कार्यालयों दो स्वंतत्र नेटवर्कों यानि इंटरनेट [7] और इंट्रांनेट [8] को बनाए रखेंगे । दोनों नेटवर्कों के बीच भौतिक रूप से कोई कनेक्शन/उपकरण नहीं होंगे । ऐसे नियोजनों में प्रयोक्ताओं के पास दो एक्सेस डिवाइसें यानि डेस्कटॉप होंगे । एक को इंटरनेट से और दूसरे को इंट्रानेट से जोड़ा जाएगा । डेटा तक गैर-प्राधिकृत एक्सेस को रोकने के लिए दोनों नेटवर्कों पर एन्ड प्वाइंट कॉम्प्लीएन्स [9] का कार्यान्वयन किया जाएगा ।

ग) प्रयोगक्ता नेटवर्क की फिल्टरिंग से बचने या अन्य किसी ऐसी गतिविधियों को करने जो नेटवर्क के प्रदर्शन या सुरक्षा को नुकसान कर सकती हैं, के लिए किसी वेबसाइट या एप्लीकेशनों के माध्यम से कोई गतिविधि नहीं करेंगे ।

5.2 सरकारी वायरलैस नेटवर्क तक पहुंच

सरकारी वायरलैस [10] नेटवर्क से जुड़ने के लिए प्रयोक्ता निम्नलिखित को सुनिश्चित करें:

क) कोई प्रयोक्ता एक्सेस डिवाइस को रजिस्टर करेगा और सरकारी वायरलैस नेटवर्क से एक्सेस डिवाइस जोड़े से पहले सक्षम प्राधिकारी से एक बारगी अनुमोदन प्राप्त करेगा।

ख) वायरलैस क्लाइंट प्रणालियों और वायरलैस डिवाइसों को अपेक्षित अधिप्रमाणन के बिना सरकारी वायरलैस एक्सेस प्वाइंट से जोड़ने की अनुमति नहीं दी जाएगी।

ग) सूचना सुरक्षा को सुनिश्चित करने क लिए यह सिफारिश की गई है कि प्रयोक्ता अपने उपकरण असुरक्षित वायरलैस नेटवर्कों के साथ नहीं जोड़ेंगे ।

5.3 साइटों की फिल्टरिंग और ब्लॉकिंग:

क) कार्यान्वयन एजेंसी, इंटरनेट पर उपलब्ध उस सूचना सामग्री को ब्लॉक करें जिसमें आईटी अधिनियम, 2000 के संबंधित प्रावधानों या अनुप्रयोग्य कानूनों का उल्लंघन किया गया हो या जिससे नेटवर्क को सुरक्षा संबंधी खतरा हो ।

ख) कार्यान्वयन एजेंसी उस सामग्री को भी ब्लॉक करेगा जो संबंधित संगठन की दृष्टि से अनुपयुक्त है या प्रयोक्ताओं की उत्पादकता को बुरी तरह प्रभावित करे।

6. मॉनीटरन और गोपनीयता:

6.1 कार्यान्वयन एजेंसी के पास इस नीति के अनुपालन की दृष्टि से निरंतर अवधि पर नेटवर्कों और् प्रणालियों की लेखा परीक्षा करने का अधिकार होगा ।

6.2 सुरक्षा संबंधी कारणों से या अनुप्रयोज्य कानूनों के अनुपालन के लिए कार्यान्वयन एजेंसी/नोडल एजेंसी, प्रयोक्ता को सूचित करने के उपरांत सरकार द्वारा उपलब्ध कराई गई डिवाइसों पर हुए किसी प्रकार के इलेक्ट्रॉनिक पत्राचार या संग्रह की गई फाइलों तक न तो पहुंच बना सकता है, न ही उनका पुनरावलोकन कर सकता है और न ही उसे कॉपी या डिलीट कर सकता है । इसमें फाइल, ई-मेल और इंटरनेट हिस्ट्री इत्यादि जैसी चीजें शामिल हैं । .

6.3 कार्यान्वयन एजेंसी सरकारी नेटवर्क पर प्रयोक्ता की ऑनलाइन गतिविधियों की मॉनीटरी करें, बशर्तें कि इस संबंध में संगठन के तौर पर ऐसी मानक प्रचालन प्रक्रियाएं बताई जाएं।

7. सरकारी नेटवर्क से ई-मेल तक पहुंच

7.1. प्रयोगक्ता सरकारी नेटवर्क से निजी ई-मेल सर्वरों को इस्तेमाल नहीं करेंगे ।

7.2. सरकारी द्वारा प्राधिकृत और कार्यान्वयन एजेंसी द्वारा कार्यान्वित ई-मेल सेवा का प्रयोग सभी प्रकार के कार्यालयी पत्राचार के लिए ही किया जाएगा । निजी पत्राचार के लिए, प्रयोक्ता सरकार द्वारा प्राधिकृत ई-मेल सेवा पर दी गई नाम आधारित ई-मेल आईडी का प्रयोग करें ।

7.3. इस संबंध में और अधिक विवरण " भारत सरकार की ई-मेल नीति" में दिए गए हैं ।

8. **सरकारी नेटवर्क से सोशल मीडिया साइटों तक पहुंच**

8.1 सरकारी संगठनों द्वारा सोशल नेटवर्किंग साइटों के प्रयोग का संचालन http://deity.gov.in. पर उपलब्ध "सरकारी संगठनों के लिए सोशल मीडिया [11] का इस्तेमाल के लिए फ्रेमवर्क और दिशानिर्देश" द्वारा संचालित है ।

8.2 प्रयोक्ता सोशल नेटवर्किंग साइटों पर सरकार से संबंधित किसी डेटा को पोस्ट करते समय आईटी अधिनियम, 2000, के तहत लागू प्रावधानों को पूरा करेगा ।

8.3 प्रयोक्ता, संबधित सोशल मीडिया प्लेटफॉर्म/वेबसाइट के साथ-साथ कॉपीराइट, निजता, मानहानि, न्यायालय की अवमानना, भेदभाव, उत्पीड़न और अन्य लागू कानूनों की "उपयोग शर्तों" का अनुपलान करेगा ।

8.4 प्रयोक्ता सक्षम प्राधिकारी को जितनी जल्दी संभव हो किसी संदिग्ध घटना के विषय में रिपोर्ट करेगा ।

8.5 प्रयोकत् हमेशा सोशल नेटवर्किंग साइटों पर उच्च सुरक्षा व्यवस्थाओं का प्रयोग करेगा।

8.6 प्रयोक्ता, अपमानजनक, धमकाने वाला, अश्लील, कॉपीराइट का उल्लंघन करने वाला, निदांत्मक, विद्वेषपूर्ण, उत्पीड़न करने वाला, भयभीत करने वाला, भेदमूलक, जाति आधारित, लिंग आधारित या किसी भी प्रकार से गैर-कानूनी सूचना सामग्री को पोस्ट नहीं करेगा । .

8.7 प्रयोक्ता, संगठन के एक कर्मचारी/कॉन्ट्रेक्टर [12] होने की हैसियत से प्राप्त गोपनीय सूचना को उजागर या इस्तेमाल नहीं करेगा ।

8.8 प्रयोक्ता किसी भी प्रकार की ऐसी टिप्पणी नहीं करेगा या ऐसी किसी भी सूचना सामग्री को पोस्ट नहीं करेगा जिससे संगठन की प्रतिष्ठा को किसी भी प्रकार से हानि हो सकती है।

9. भारत सरकार द्वारा किसी प्रयोक्ता को जारी आईटी उपकरण

आईटी उपकरणों का प्रयोग प्राथमिकता रूप से सरकारी संबंधी उद्देश्यों केलिए और कानूनी और नीतिपरक रूप से किया जाएगा और उनका संचाल शीर्षक "आईटी संसाधनों के इस्तेमाल पर नीति" शीर्षक के अंतर्गत http://www.deity.gov.in/content/ policiesguidelines/ पर उपलबंध "सरकारी नेटवर्क पर आईटी उपकरणों के इस्तेमाल पर दिशानिर्देश" दस्तावेज में निर्धारित पद्धतियों द्वारा किया जाएगा। उपरोक्त दस्तावेज में डेस्कटॉप उपकरण, पोर्टेबल उपकरणों, बाह्य स्टोरेज मीडिया और प्रिंटर और स्कैनर जैसे पैरिफेरल उपकरण शामिल हैं।

10. प्रयोक्ता संगठनों की जिम्मेदारी

10.1. नीति अनुपालन

क) सभी प्रयोक्ता संगठन, अपने प्रयोक्ताओं द्वारा इस नीति के साथ अनुपलान सुनिश्चित करने के लिए पर्याप्त नियंत्रण लागू करें।

ख) इस नीति का अनुपलान सुनिश्चित करने के लिए संगठन के सक्षम प्राधिकारी द्वारा आवधिक रिपोर्टिंग आवश्यकता को पूरा किया जाएगा।

ग) नोडल अधिकारी अपने प्रयोक्ताओं द्वारा इस नीति में निहित सुरक्षा संबंधी पक्षों से संबंधित सभी घटनाओं के समाधान को सुनिश्चित करेगा। इस संबंध में कार्यान्वयन एजेंसी अपेक्षित सहयोगी उपलब्ध कराएगी।

घ) प्रयोक्ता संगठन का सक्षम प्राधिकारी यह सुनिश्चित करेगा कि आईटी संसधानों के प्रयोग पर प्रशिक्षण और जागरूकता कार्यक्रमों का आयोजन नियमित अवधि पर किया जाए। कार्यान्वयन एजेंसी इससंबंध में आवश्यक सहायता मुहैया कराएगी।

ङ) प्रयोक्ता संगठन कार्यान्वयन एजेंसी के साथ परामर्श किए बिना नेटवर्क पर किसी भी प्रकार के नेटवर्क/सुरक्षा उपकरण को इंस्टॉल नहीं करेगी।

10.2. **नीति का प्रचार-प्रसार**

क) प्रयोक्ता संगठन का सक्षम प्राधिकारी यह सुनिश्चित करेगा कि इस नीति का समुचित रूप से प्रचार-प्रसार।

ख) सक्षम प्राधिकारी अपने प्रयोक्ताओं के बीच इस नीति के बारे जानकारी बढ़ाने के लिए न्यूजलैटर, बैनर, बुलिटिन बोर्ड इत्यादि का प्रयोग कर सकता है।

ग) नये भर्ती किए गए कर्मचारियों के लिए ओरिएन्टेशन कार्यक्रमों में इस नीति पर एक सत्र शामिल होगा।

11. सुरक्षा घटना प्रबंधन प्रक्रिया

11.1 एक सुरक्षा घटना को एक विपरीत घटना के तौर पर परिभाषित किया गया है जो सरकारी डेटा की उपलब्धता, अखण्डता, गोपनीयता और प्राधिकारी को प्रभावित कर सकती है।

11.2 कार्यान्वयन एजेंसी के पास उस संगठन के सक्षम प्राधिकारी को सूचित करके ऐसे किसी भी उपकरण को निष्क्रिय कर हटाने का अधिकार है, जो खतरनाक हो सकती है और प्रणाली के लिए नुकसान देह हो सकती है।

11.3 नोटिस में लाई गई किसी भी सुरक्षा घटना [13] को त्वरित भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (आई-सर्ट) और कार्यान्वयन एजेंसी की नजर में लाया जाए।

12. छंटाई/लॉग जारी करना

12.1 उपरोक्त खंड में दिए गए किसी भी प्रावधान के न होते हुए भी कार्यान्वियन एजेंसी द्वारा कानून प्रवर्तन एजेंसियों और अन्य संगठनों के समक्ष उसी आईटी संसाधन से संबंधित या उसमें निहित लॉग का प्रकटन आईटी अधनियम 2000 और अन्य लागू कानूनों के अनुसार किया जाएगा।

12.2 कार्यान्वियन एजेंसी लॉग की जांच करने या जारी करने के लिए जारी करने के लिए जब तक इस खंड में प्रावधान न किया जाए किसी अन्य संगठन से प्राप्त अनुरोध को न तो स्वीकार करेगा और न ही उस पर कार्यवाही करेगा।

13. बौद्धिक संपदा

कार्यान्वियन एजेंसी नेटवर्क और संसाधनों के माध्यम से प्राप्त सामग्री की सुरक्षा कॉपीराइट और पेटेन्ट, ट्रेडमार्क, व्यापार भेदों या गोपनीयता, प्रसारण या अन्य निजी अधिकार और बौद्धिक संपदा अधिकार स्वामित्व संबंधी अन्य सूचना की सुरक्षा हेतु कानूनों समेत, पर इन तक सीमित नहीं, के अधीन होगी। प्रयोक्ता किसी भी तरीके से सरकारी नेटवर्क और संसाधनों का प्रयोग इस प्रकार नहीं करेंगे जिससे ऐसे अधिकारों का प्रभाव, दुरूपयोग हो या अन्यथा उल्लंघन हो।

14. प्रवर्तन

14.1 यह नीति केन्द्र सरकार और राज्य सरकार के सभी कार्मचारियों पर लागू है, जैसा कि इस दस्तावेज के खंड 2 में निर्दिष्ट किया गया है। सभी प्रयोक्ताओं के लिए इस नीति के प्रावधानों का अनुपलान अनिवार्य है।

14.2 प्रत्येक संगठन इस नीति के प्रावधानों के अनुपालन को सुनिश्चित करने के लिए जिम्मेदार होगी। कार्यान्वियन एजेंसी इस संबंध में संगठनों को आवश्यक तकनीकी सहायता उपलब्ध कराएगी।

15. डीएक्टीवेशन

15.1. प्रयोक्ता द्वारा उपयोग किए जा रहे संसाधनों से सरकारी प्रणालियों या नेटवर्क की सुरक्षा को होने वाले खतरे के मामले में, उपयोग किए जा रहे संसाधनों को कार्यान्यिवन एजेंसी द्वारा तुरंत डीएक्टीवेट किया जाए।

15.2. ऐसे डीएक्टीवेशन के बाद उस संगठन के सक्षम प्राधिकारी और संबंधित प्रयोक्ता को सूचित किया जाएगा।

16. **एनआईसी नेटवर्क अवसंरचना की लेखापरीक्षा**

डीईआईटीवाई द्वारा अनुमोदित संगठन द्वारा एनआईसी नेटवर्क अवसंरचना की सुरक्षा लेखा परीक्षा का संचालन आवधिक रूप से किया जाएगा।

17. 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.	शब्दावली	परिभाषा
1	प्रयोक्ता	प्रयोक्ता से सरकार/राज्य/संघ राज्य क्षेत्र के कर्मचारियों/संविदा आधार पर कार्यरत कर्मचारियों से अभिप्रेत है जो सरकारी सेवाओं का लाभ उठा रहे हैं।
2	संगठन	केन्द्र और राज्य सरकार के अंतर्गत मंत्रालय/विभाग/सांविधिक निकाय/स्वायत्त निकाय
3	सक्षम प्राधिकारी	सक्षम प्राधिकारी से अपने संगठन में इस नीति से संबधित सभी निर्णय लेने और अनुमोदित करने के लिए जिम्मेदार अधिकारी से अभिप्रेत है।

4.	नोडल अधिकारी	नोडल अधिकारी से इस नीति संबंधी सभी मुद्दों के लिए जिम्मेदार अधिकारी जो संगठन की तरफ से इसका समन्वय करेगा ।
5	कार्यान्वयन एजेंसी (आईए)	कार्यान्वयन एजेंसी (आईए) से इस नीति में यथा निर्दिष्ट एहतियाती और दण्डनीय कार्रवाई करने की शक्ति समेत नेटवर्क सेवाओं के संदर्भ में इस नीति का अनुपालन सुनिश्चित करने के लिए जिम्मेदार निकाय अभिप्रेत है ।
6	नोडल एजेंसी	नोडल एजेंसी से नेटवर्क सेवाओं को छोड़कर आईटी संसाधनों के इस्तेमाल के संबंध में इस नीति का अनुपालन सुनिश्चित करने के लिए जिम्मेदार संगत संगठन अभिप्रेत है ।
7	इंटरनेट	इंटरनेट विश्वव्यापी स्तर पर आपस में जुड़े कम्प्यूटर नेटवर्किंग का एक नेटवर्क है, जोकि आम जनता की पहुंच में है । आपस में जुड़े ये कम्प्यूटर विशेष प्रकार की पैक्डस्विचिंग जिसे आईपी या इंटरनेट प्रोटोकॉल कहा जाता है के माध्यम से डेटा ट्रांसमिशन द्वारा काम करते हैं ।
8	इंट्रानेट	इंट्रानेट एक निजी नेटवर्क होता है जो किसी संगठन के भीतर निहित होता है । इस नीति के प्रयोजन से किसी इंट्रानेट से जुड़े कम्प्यूटरों को इंटरनेट से जोड़ने की अनुमति नहीं होती है ।
9	अंतिम बिंदु अनुपालन	अंतिम बिन्दु अनुपालन नेटवर्क संरक्षण का एक तरीका है जिसमें अपेक्षा की गई है कि नेटवर्क से जुड़े प्रत्येक कम्प्यूटिंग उपकरण, नेटवर्क एक्सेस मिलने से पहले कुछ मानकों को पूरा करे । अंतिम बिंदुओं में डेस्कटॉप, लैपटॉप, स्मार्ट फोन, टेबलेट इत्यादि शामिल हो सकते हैं।
10	वायरलैस	नेटवर्क नोडों को जोड़ने के लिए वायरलैस डेटा कनेक्शन का प्रयोग करने वाला एक प्रकार का कम्प्यूटर नेटवर्क । इस नीति के उददेश्य से, भारत सरकार के सभी वायरलैस नेटवर्कों का नियोजन सुरक्षित ढंग से किया जाएगा ।
11	सोशल मीडिया	सोशल मीडिया का अर्थ उन सोशल नेटवर्किंग साइटों, ब्लॉग, इलेक्ट्रॉनिक न्यूजलैटरों, ऑनलाइन फोरमों, सोशल नेटवर्किंग साइटों और अन्य सेवाओं से है जो प्रयोक्ताओं का समकालीन रूप से अन्य प्रयोक्ताओं के साथ सूचना साझा करने की सुविधा उपलब्ध कराना है।
12	संविदाकार, संविदा आधारित कर्मचारी	कर्मचारी जो संविदा आधार पर भारत सरकार के लिए कार्य करता है/संविदा आधारित कर्मचारी को एक विशिष्ट कार्य के लिए रखा जाता है । संविदा आधारित कर्मचारी भारत सरकार के स्टाफ का नियमित कर्मचारी नहीं होता है और उसे भारत सरकार का स्थायी कर्मचारी नहीं माना जाता ।
13	सुरक्षा घटना	सरकारी डेटा के साथ हुई किसी भी प्रकार की छेड़छाड और उससे उत्पन्न सुरक्षा संबंधी खतरा/डेटा उल्लंघन

MINISTRY OF COMMUNICATION AND INFORMATION TECHNOLOGY

(Department of Electronics and Information Technology)

NOTIFICATION

New Delhi, the 18th February, 2015

Subject: Policy on use of IT Resources of Government of India

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

1.1 Government provides IT resources to its employees to enhance their efficiency and productivity. These resources are meant as tools to access and process information related to

their areas of work. These resources help Government officials to remain well informed and carry out their functions in an efficient and effective manner.

1.2 For the purpose of this policy, the term 'IT Resources' includes desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

1.3 Misuse of these resources can result in unwanted risk and liabilities for the Government. It is, therefore, expected that these resources are used primarily for Government related purposes and in a lawful and ethical way.

2. Scope

This policy governs the usage of IT Resources from an end user's [1] perspective**.** This policy is applicable to all employees of GoI and employees of those State/UT Governments that use the IT Resources of GoI and also those State/UT Governments that choose to adopt this policy in future**.**

3. Objective

The objective of this policy is to ensure proper access to and usage of Government's IT resources and prevent their misuse by the users. Use of resources provided by Government of India (GoI) implies the user's agreement to be governed by this policy.

4. Roles and Responsibilities

The following roles are required in each organization [2] using the Central / State / UT Government IT resources. The official identified for the task shall be responsible for the management of the IT resources deployed for the use of entire user base under their respective domain.

4.1 Competent Authority [3] as identified by each organization.

4.2 Designated Nodal Officer [4] as identified by each organization.

4.3 Implementing Agency [5]: The overall responsibility for Information Security will be that of the respective organization. In the interest of security of the network services, it is recommended that the organizations should use the GoI network services provided by NIC, in which case NIC would be the Implementing Agency for security of network services on behalf of the concerned organization. In organizations not using NIC network services, the respective organization will be the Implementing Agency.

4.4 The Nodal Agency [6] for managing all IT Resources except network services shall be the respective organization.

5. Access to the Network

5.1. ***Access to Internet and Intranet***

a) A user shall register the client system and obtain one time approval from the competent authority before connecting the client system to the Government network.

b) It is strongly recommended that sensitive offices shall maintain two independent networks, i.e. Internet [7] and Intranet [8]. Both the networks shall not have any physical connection/devices between them. Users in such deployments shall have two access devices, i.e. desktops. One shall be connected to the internet and the other to the intranet. End point compliance [9] shall be implemented on both the networks to prevent unauthorised access to data.

c) Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

5.2 Access to Government Wireless Networks

For connecting to a Government wireless [10] network, user shall ensure the following:—

a) A user shall register the access device and obtain one time approval from the competent authority before connecting the access device to the Government wireless network.

b) Wireless client systems and wireless devices shall not be allowed to connect to the Government wireless access points without due authentication.

c) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

5.3 Filtering and blocking of sites:

a) IA may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 and other applicable laws or which may pose a security threat to the network.

b) IA may also block content which, in the opinion of the organization concerned, is inappropriate or may adversely affect the productivity of the users.

6. Monitoring and Privacy:

6.1 IA shall have the right to audit networks and systems at regular intervals, from the point of compliance to this policy.

6.2 IA/Nodal Agency, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on Government provided devices under intimation to the user. This includes items such as files, e-mails, and Internet history etc.

6.3 IA may monitor user's online activities on Government network, subject to such Standard Operating Procedures as the organization may lay down in this regard.

7. E-mail Access from the Government Network

7.1 Users shall refrain from using private e-mail servers from Government network.

7.2 E-mail service authorized by the Government and implemented by the IA shall only be used for all official correspondence. For personal correspondence, users may use the name-based e-mail id assigned to them on the Government authorized e-mail Service.

7.3 More details in this regard are provided in the "E-mail Policy of Government of India".

8. Access to Social Media Sites from Government Network

8.1 Use of social networking sites by Government organizations is governed by "Framework and Guidelines for use of Social Media [11] for Government Organizations" available at http://deity.gov.in.

8.2 User shall comply with all the applicable provisions under the IT Act, 2000, while posting any data pertaining to the Government on social networking sites.

8.3 User shall adhere to the "Terms of Use" of the relevant social media platform/website, as well as copyright, privacy, defamation, contempt of court, discrimination, harassment and other applicable laws.

8.4 User shall report any suspicious incident as soon as possible to the competent authority.

8.5 User shall always use high security settings on social networking sites.

8.6 User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

8.7 User shall not disclose or use any confidential information obtained in their capacity as an employee/contractor [12] of the organization.

8.8 User shall not make any comment or post any material that might otherwise cause damage to the organization's reputation.

9. Use of IT Devices Issued by Government of India

IT devices issued by the Government to a user shall be primarily used for Government related purposes and in a lawful and ethical way and shall be governed by the practices defined in the document **"Guidelines for Use of IT Devices on Government Network"** available at http://www.deity.gov.in/content/policiesguidelines/ under the caption "Policy on Use of IT Resources". The aforesaid document covers best practices related to use of desktop devices, portable devices, external storage media and peripherals devices such as printers and scanners.

10. Responsibility of User Organizations

10.1. Policy Compliance

a) All user organizations shall implement appropriate controls to ensure compliance with this policy by their users. Implementing Agency shall provide necessary support in this regard.

b) A periodic reporting mechanism to ensure the compliance of this policy shall be established by the competent authority of the organization.

c) Nodal Officer of the user organization shall ensure resolution of all incidents related to the security aspects of this policy by their users. Implementing Agency shall provide the requisite support in this regard.

d) Competent Authority of the user organization shall ensure that training and awareness programs on use of IT resources are organized at regular intervals. Implementing Agency shall provide the required support in this regard.

e) User organization shall not install any network/security device on the network without consultation with the IA.

10.2. Policy Dissemination

a) Competent Authority of the user organization should ensure proper dissemination of this policy.

b) Competent Authority may use newsletters, banners, bulletin boards etc. to facilitate increased awareness about this policy amongst their users.

c) Orientation programs for new recruits shall include a session on this policy.

11. Security Incident Management Process

11.1 A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Government data.

11.2 IA reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of that organization.

11.3 Any security incident [13] noticed must immediately be brought to the notice of the Indian Computer Emergency Response Team (ICERT) and the IA.

12. Scrutiny/Release of logs

12.1 Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law Enforcement agencies and other organizations by the IA shall be done as per the IT Act, 2000 and other applicable laws.

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

13. Intellectual Property

Material accessible through the IA's network 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 network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

14. Enforcement

14.1 This policy is applicable to all employees of Central and State Governments as specified in clause 2 of this document. It is mandatory for all users to adhere to the provisions of this policy.

14.2 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.

15. Deactivation

15.1. In case of any threat to security of the Government systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the IA.

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

16. Audit of NIC Network Infrastructure

The security audit of NIC network infrastructure shall be conducted periodically by an organization approved by Deity.

17. 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/contractual employees who are accessing the Government services.
2	**Organization**	Ministry/Department/Statutory Body/Autonomous body under Central and State Governments.
3	**Competent Authority**	Officer responsible for taking and approving all decisions relating to this policy in his Organization.
4.	**Nodal Officer**	Officer responsible for all matters relating to this policy who will coordinate on behalf of the Organization.
5	**Implementing Agency (IA)**	A Body which will be responsible for ensuring compliance with this policy with reference to network services including power to take precautionary and penal actions as specified in this policy.
6	**Nodal Agency**	Respective organization responsible for ensuring compliance with this policy with respect to use of It resources except network services.

7	**Internet**	Internet is a network of the interlinked computer networking worldwide, which is accessible to the general public. These interconnected computers work by transmitting data through a special type of packet switching which is known as the IP or the internet protocol.
8	**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.
9	**End point compliance**	End point compliance is an approach to network protection that requires each computing device on a network to comply with certain standards before network access is granted. Endpoints can include desktops, laptops, smart phones, tablets etc .
10	**Wireless**	Any type of computer network that uses wireless data connections for connecting network nodes. For the purpose of this policy, all the GoI wireless networks will be deployed in a secure manner.
11	**Social Media**	Applies to social networking sites, blogs, electronic newsletters, online forums, social networking sites, and other services that permit users to share information with others in a contemporaneous manner.
12	**Contractor/contractual employees**	An employee who works under contract for GoI. A contract employee is hired for a specific job or assignment. A contract employee does not become a regular addition to the GoI staff and is not considered a permanent employee of GoI.
13	**Security Incident**	Any adverse event which occurs on any part of the government data and results in security threat/breach of the data.

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