प्रयोगकर्ता हेतु सुरक्षा नीति

1.उद्देश्य: नीति का उद्देश्य सुरक्षित एवं स्वीकार योग्य ग्राहक पद्धति के प्रयोग को उपलब्ध कराना।

2.क्षेत्र: मंत्रालय/विभाग/भारत सरकार के संबद्ध कार्यालयों के कर्मचारियों को अवर्गीकृत सूचनाओं के संचालन हेतु यह नीति लागू है।

3.अपवाद प्रबंधन: किसी भी प्रकार के अपवाद/परिवर्तन, प्रयोगकर्ता मुख्य सूचना सुरक्षा अधिकारी से अनुमोदन ले सकते है।

4.नीति

4.1 ग्राहक पद्धति के स्वीकार्य उपयोग

4.1.1 ग्राहक पद्धति पर उन्हें आवंटित खाते पर गतिविधि प्रयोग हेतु प्रयोगकर्ता उत्तरदायी होगा।

4.1.2 अनुविक्षण/विद्वेशपूर्ण हेतु निस्पंदन/अनधिकृत गतिविधि की शर्त पर प्रयोगकर्ता नेटवर्क पहुंच।

4.1.3 ग्राहक पद्धति पर किसी भी प्रकार के प्रशासनिक गतिविधि हेतु प्रयोगकर्ता पद्धति प्रशासन हेतु सुरक्षा नीति का अनुसरण करेगा।

4.1.4 प्रयोगकर्ता ग्राहक पद्धति पर सीमित सुविधा के साथ खाते का प्रयोग करेगा तथा प्रशासनिक सुविधा को प्रयोग नहीं करेगा।

4.1.5 प्रयोगकर्ता द्वारा नियमित अंतराल में महत्वपूर्ण फाइलों का बैक-अप लिया जाएगा।

4.1.6 पद्धति/मीडिया से संबंधित कार्यालय सूचना प्रत्यक्ष रूप से सुरक्षित किया जाएगा।

4.1.7 उपस्थित रहित पद्धति को प्रयोगकर्ता नहीं छोड़ेगा। प्रयोगकर्ता पद्धति को छोड़ने से पहले अपनी पद्धति को बंद करेगा। अतिरिक्त रूप से ग्राहक पद्धति पर आदर्श पद्धति के समनुरूप समय लेगा।

4.1.8 ग्राहक पद्धति में दोषों के रख रखाव या पिरहार प्रयोगकर्ता के देख रेख के अन्तर्गत होगा।

4.1.9 उपयोगकर्ता यह सुनिश्चित करें कि सिस्टम का समय भारतीय मानक समय के अनुसार हो। किसी भी प्रकार के परिवर्तन की सूचना सिस्टम एडमिनिस्टेटर/नेटवर्क सुरक्षा एडमिनिस्टेटर को दी जाएगी।

4.1.0 उपयोगकर्ता निम्नलिखित में से किसी भी गतिविधि में लिप्त नहीं होना चाहिए:

4.1.10.1 सुरक्षा उपायों की अवहेलना करना।

4.1.10.2 सिस्टम/डाटा/प्रोग्राम अनाधिकृत तरीके से एक्सेस करना।

4.1.10.3 सुरक्षा उपायों की अवहेलना करना।

4.1.10.4 किसी भी रूप में राष्ट्र विरोधी, अपराधिक, मानहानिकारक, विभेदक, दुर्भावनापूर्ण अथवा प्रोनोग्राफिक सामग्री बनाना, एक्सेस करना, क्रियान्वित करना, डाउनलोड करना, वितरण करना, स्टोर करना अथवा प्रदर्शित करना।

4.1.10.5 अनाधिकृत प्रयोग के लिए साफ्टवेयर/डाटा की प्रतियां निर्मित करना।

4.1.10.6 प्रतिरूपण करना।

4.1.10.7 फिशिंग।

4.1.10.8 सोशल इंजीनियरिंग।

4.1.10.9 सॉफ्टवेयर लाइसेंस का अनाधिकृत प्रयोग।

4.1.10.10 इंटरनेट मेल समूह/बुलेटिन बोर्ड को व्यक्तिगत प्रयोग के लिए कार्यालयी ई-मेल का पता उपलब्ध कराना।

4.1.10.11 ऐसी कोई भी गतिविधि जोकि केन्द्रीय सिविल सेवा (आचरण) नियमों का उल्लंघन करती है।

4.1.11 उपयोगकर्ता सुरक्षा घटनाक्रम की सूचना सिस्टम एडमिनिस्टेटर/नेटवर्क सुरक्षा एडमिनिस्टेटर को प्रदान करें।

4.1.12 उपयोगकर्ता यह सुनिश्चत कर लें कि अनाधिकृत पियर टू पियर फाइल शेयरिंग साफ्टवेयर इंस्टाल नहीं किया गया है।

4.1.13 उपयोगकर्ता यह सुनिश्चित कर लें कि सिस्टम निम्नानुसार कॉन्फ़िगर किया गया है।

4.1.13.1 उपयोगकर्ता किसी के भी साथ बाय डिफाल्ट क्लाइंट सिस्टम शेयर नहीं करेंगे। यद्यपि आवश्यकता एवं कारण विशेष होने पर जैसे (क्लाइंट सिस्टम शिफ्ट ड्यूटी में प्रयुक्त किया जा रहा हो) निम्नलिखित को सुनिश्चित किया जाए:

4.1.13.1.1 प्रत्येक क्लाइंट सिस्टम एवं इसका उपयोग करने वाले प्रत्येक उपयोगकर्ता के लिए सक्षम/नामित प्राधिकारी से स्पष्ट अनुमोदन प्राप्त किया जाए।

4.1.13.1.2 शेयरड् क्लाइंट सिस्टम को उपयोग करने के लिए प्रत्येक उपयोगकर्ता हेतु अलग खाता होगा।

4.1.13.1.3 फाइल/फोल्डर उपयोग करने हेतु अनुमति केवल आवश्यक कार्यों तक सीमित होगी।

4.1.13.2 उपयोगकर्ता किसी के भी साथ हार्ड डिस्क अथवा फोल्डर शेयन नहीं करेंगे। यद्यपि आवश्यकता होने पर जैसे केवल आवश्यक फोल्डर किसी भी निर्धारित प्रयोगकर्ता के साथ शेयर किए जाऐंगें।

4.1.13.3 क्लाइंट सिस्टम में क्लाइंट सिस्टम सुरक्षा (सीएसएस) का प्रयोग क्लाइंट सिस्टम सुरक्षा निर्देशों के अनुसार किया गया है।

4.1.13.4 क्लाइंट सिस्टम के सभी इंटरफेस के स्थान पर केवल वे इंटरफेस कार्य करेंगें जिनकी आवश्यकता हो। कंफिगरेशन के लिए उपयोगकर्ता सिस्टम एडमिनिस्टेटर से संपर्क कर सकते हैं।

4.2 वायरस एवं दोषपूर्ण कोड (एडवेयर, स्पायवेयर, मैलवेयर)

4.2.1 उपयोगकर्ता यह सुनिश्चित करलें कि सिस्टम प्राधिकृत एन्टी वायरस सॉफ्टवेयर से कंफिगर किया गया हो।

4.2.2 उपयोगकर्ता यह सुनिश्चित करें कि एन्टी वायरस सॉफ्टवेयर एवं वायरस पैर्टन फाइल अद्यतन हों।

4.2.3 उपयोगकर्ता यह सुनिश्चित करें कि एन्टी वायरस स्कैन नियमित अंतराल के बाद कंफिगर हो।

4.2.4 यदि वायरस क्लीन नहीं होता है तो इस संबंध में सिस्टम एडमिनिस्टेटर/नेटवर्क सिक्युरिटी एडमिनिस्टेटर को सूचित किया जाए।

4.3 हार्डवेयर, प्रचालन पद्धति एवं एप्लीकेशन सॉफ्टवेयर

4.3.1 उपयोगकर्ता केवल वे ही साफ्टवेयर/हार्डवेयर प्रयोग करेंगे जोकि विभाग द्वारा अधिकृत किए गए हैं।

4.3.2 निम्नलिखित कार्य सिस्टम एडमिनिस्टेटर द्वारा किए जाऐंगे जबकि उपयोगकर्ता को यह सुनिश्चित कर लेना चाहिए कि:

4.3.2.1 आपरेटिंग सिस्टम एवं अन्य सॉफ्टवेयर अधिकृत माध्यम/ऐसे उपकरण निर्माता (ओईएम) जिनके पास वैध लाइसेंस हो के माध्यम से ही इंस्टाल किए जाऐं।

4.3.2.2 ऑपरेटिंग सिस्टम एवं अन्य साफ्टवेयर पैकेज इंस्टाल करते समय आवश्यक उपयोगिताऐं ही इंस्टाल की जाऐं।

4.3.2.3 उपलब्ध नवीनतम सर्विस पैक, पैचेस एवं ड्राइवर्स ही इंस्टाल किए जाऐं।

4.3.2.4 रिमूवेबल मीडिया से बूटिंग वर्जित है।

4.3.2.2 सभी रिमूवेबल ड्राइव पर आटो रन वर्जित है।

4.3.2.2 पैच सर्वर द्वारा उपलब्ध कराए जाने वाले सर्विस पैक एवं पैचेस इंस्टाल करने के लिए उपयोगकर्ता द्वारा अनुमति दी जाए।

4.4 ई-मेल उपयोग

4.4.1 विभाग द्वारा दिए गए ई-मेल का प्रयोग केवल कार्यालयीन संप्रेषण के लिए किया जाए।

4.4.2 कार्यालयीन ई-मेल व्यक्तिगत ई-मेल खाते में अग्रसारित न किए जाऐं।

4.4.3 ई-मेल पासवर्ड कार्यालयीन प्रयोग के लिए भी किसी को न बताऐं।

4.4.4 उपयोगकर्ता द्वारा ई-मेल किसी भी प्रकार से अनाधिकृत प्रयोग करने का प्रयास न किया जाए, जैसे:

4.4.4.1 अनाम रूप से संदेशों का वितरण।

4.4.4.2 अन्य प्रयोगकर्ताओं के ई-मेल पते का अनुचित प्रयोग।

4.4.4.3 अवास्तविक पहचान का प्रयोग ।

4.4.4.4 दूसरों को परेशान एवं भयभीत करने हेतु संदेशों का प्रेषण।

4.4.5 ऑनलाइन आवेदन/सेवा/पंजीकरण/न/सेवा/पंजीकरण/सदस्यता हेतु आवेदन करते समय पासवर्ड कार्यालयीन ई-मेल खाते के पासवर्ड के समान नहीं होना चाहिए।

4.5 पासवर्ड सुरक्षा

4.5.1 पासवर्ड का चयन पासवर्ड मैनेजमैंट गाइडलाइन के अनुसार किया जाए।

4.5.2 निम्नलिखित कार्य सिस्टम एडमिनिस्टेटर द्वारा किए जाऐंगे जबकि उपयोगकर्ता को यह सुनिश्चित कर लेना चाहिए कि:

4.5.2.1 पासवर्ड बीआईओएस, सिस्टम लॉगिन एवं स्क्रीनसेवन स्तर पर किए जाए।

4.5.2.2 क्लाइंट सिस्टम में आटो लोगोन फीचर उपलब्ध नहीं है।

4.5.2.3 असफल प्रवेश की पूर्वनिर्धारित संख्या समाप्त होने पर उपयोगकर्ता का खाता लॉक कर दिया जाएगा।

4.5.3 उपयोगकर्ता पासवर्ड किसी को नहीं बताऐंगे।

4.5.4 पासवर्ड मैनेजमैंट गाइडलाइन के अनुसार पासवर्ड नियमित अंतराल के बाद बदल दिए जाने चाहिए।

4.5.5 यदि यह पाया जाता है कि पासवर्ड किसी को बताया गया है/किसी के साथ साझा किया गया है तो उसे तुरंत बदला जाए तथा घटना की सूचना सिस्टम एडमिनिस्टेटर/नेटवर्क सुरक्षा एडमिनिस्टेटर को दी जाए।

4.6 पोर्टेबल स्टोरेज मीडिया

4.6.1 उपयोगकर्ता केवल कार्यालय द्वारा जारी किए गए पोर्टेबल स्टोरज मीडिया का ही प्रयोग करेंगे।

4.6.2 उपयोगकर्ता पोर्टेबल स्टोरज मीडिया की आवश्यकता न होने पर अथवा इसके खराब होने पर/सही ढ़ंग से काम न कर पाने पर इसे वापस करेंगे।

4.6.3 उपयोगकर्ता यह सुनिश्चित करलें कि इस्तेमाल किया जाने वाला पोर्टेबल स्टोरज मीडिया वायरस रहित है।

4.6.4 उपयोगकर्ता यह सुनिश्चित करलें कि पोर्टेबल स्टोरज मीडिया से सॉफ्टवेयर का निष्पादन नहीं किया गया है।

4.7 उपयोगकर्ता के लिए लागू एक्सेस पॉलिसी

4.7.1 उपयोगकर्ता को नेटवर्क क्लाइंट सिस्टम से जुड़ने के लिए सक्षम अधिकारी से पूर्व में ही अनुमोदन प्राप्त करना होगा ।

4.7.2 वह क्लाइंट सिस्टम जो किसी एक नेटवर्क से जुड़ा हो अन्य नेटवर्क से नहीं जुड़ेगा।

4.7.3 वायरलेस कनेकटिविटी के लिए, उपयोगकर्ता को यह सुनिश्चित करना होगा कि :

4.7.3.1 वायरलेस इंटरफेस बाय डिफाल्ट निष्क्रीय है।

4.7.3.2 सक्षम अधिकारी की अनुमति के बिना वायरलेस नेटवर्क/डिवाइस क्लाइंट सिस्टम से नहीं जोड़े जा सकेंगे।

4.7.3.3 अनुमति प्राप्त होने के उपरांत क्लाइंट सिस्टम केवल प्राधिकृत वायरलेस नेटवर्क से जुड़ सकेंगे।

4.8 क्लाइंट सिस्टम लॉग

4.8.1 प्रशासनिक विशेषाधिकार प्राप्त उपयोगकर्ता क्लाइंट सिस्टम से ऑडिट चिन्ह/लॉग डिलीट नहीं कर सकेंगे।

5. समीक्षा इस सुरक्षा पॉलिसी की समीक्षा आईटी वातावरण में किसी भी प्रकार का परिवर्तन होने पर अथवा वर्ष में एक बार ,जो भी पहले हो की जाएगी । समीक्षा निम्नलिखत के आंकलन हेतु की जाएगी:

5.1 अभिनियोजित तकनीक/नेटवर्क सिक्युरिटी आर्किटेक्चर, नियोजक एवं/अथवा कानूनी आवश्यकता के अनुसार किए गए अपरिवर्तनीय परिवर्तनों का जोखिम प्रोफाइल पर प्रभाव।

5.2 सुरक्षा नियंत्रण की प्रभावकारिता का वर्णन पॉलिसी में किया गया है। समीक्षा के आधार पर वर्तमान पॉलिसी में सुधार अथवा परिवर्तन किया जा सकता है।

6. लागू होना इस पॉलिसी के नियमों को तोड़ना सीसीएस कंडक्ट नियमों के अंतर्गत नियमों का उल्लंघन माना जाएगा।