1. परिचय

1.1 सूचना सुरक्षा

सूचना सुरक्षा की सफलता सूचना की सुरक्षा के लिए बनाई जाने वाली नीतियों पर निर्भर करती है । सुरक्षा नीति में यह स्पष्ट किया जाता है कि सूचना प्रणालियों (सिस्टमों) की सुरक्षा में संस्थान किस लक्ष्य की पूर्ति करना चाहता है । इसका स्पष्ट लक्ष्य दुर्घटनावश या सप्रयास सूचना सम्पदाओं को पहुंचने वाले नुकसान को कम करने के लिए सिस्टम का प्रयोग करने वाले व्यक्ति के कार्यों को नियंत्रित या उनका मार्गदर्शन करना है ।

सूचना सुरक्षा नीतियों से सूचना संसाधनों की सुरक्षा तथा कुशलता को सुदृढ़ बनाया जाता है । ये नीतियां संस्थान सूचना सुरक्षा का प्राथमिक आधार होती हैं । हम सब अपने दैनिक जीवन में डाटा की सुरक्षा करने के अभ्यस्त होते हैं । उदाहरणार्थ, घर में हम कानूनी और बीमा के दस्तावेज संभाल कर रखते है। ताकि वे जरूरत पड़ने पर तत्काल उपलब्ध हो सकें । कार्यालय की सभी सूचनाओं को भी इसी प्रकार रखा जाना चाहिए । किसी कार्यालय में सही सूचना का मिलना इसकी सफलता का सूचक होता है । डाटा सुरक्षा से यूजर को असावधानीवश या दुर्भावना से सूचनाओं को समाप्त करने, परिवर्तन करने या अनधिकृत रूप से जानकारी प्राप्त करने पर नियंत्रण तथा सूचना सुरक्षा में सहायता मिलेगी ।
डाटा सुरक्षा के तीन पहलू हैं :–

गोपनीयता: सूचना की अनधिकृत जानकारी जैसे प्रैस आदि से बचाना या सूचना का अनुचित प्रयोग करने वालों या सूचना प्राप्त करने के पात्र न होने वाले व्यक्तियों से सूचना की सुरक्षा करना ।
सम्पूर्णता: विश्वसनीय, उपयोगी, सही और सम्पूर्ण सूचना की सुनिश्चिता के साथ–साथ अनधिकार परिवर्तनों से सूचना का बचाव ।
उपलब्धता: आवश्यकता पड़ने पर सूचना का तत्काल उपलब्ध होना ।
डाटा को अलग–अलग कई भागों में रख जा सकता है:

- नेटवर्क सर्वर
- पर्सनल कॅप्यूटर तथा नेटवर्क वर्कस्टेशन
- लैपटॉप एवं हैंडहेल्ड पीसी
- रिमूवेबल स्टोरेज मीडिया– (फलॉपी डिस्क, सीडी रॉम, जिप डिस्कस, फलेश ड्राइव इत्यादि)
- डाटा बैकअप मीडिया (टेप एवं ऑपटीक्ल डिस्क)

...2...

1.1 डाटा नुकसान से बचाव

डाटा को हानि पहुंचने के मुख्य कारण :–

- प्राकृतिक आपदा(आग, भूकम्प, बाढ़ इत्यादि)
- वायरस
- मानवीय त्रुटि (हयूमेन एरर्स)
- सॉफ्टवेयर खराबी
- हार्डवेयर तथा सिस्टम की खराबी

कम्प्यूटर एवं उसमें रखे डाटा पर हमारी निर्भरता रोज़ बढ़ती जा रही है । लगभग सभी स्थितियों में सिस्टम की मरम्मत या बदला जाना संभव है परन्तु एक बार डाटा समाप्त हो जाने पर वापिस प्राप्त नहीं किया जा सकता । इसी कारण नियमित रूप से सिस्टम बैकअप तथा कुछ सुरक्षात्मक उपाय अपनाने पर अधिक ज़ोर दिया जाता है ।

प्राकृतिक आपदा:

यद्यपि प्राकृतिक आपदाओं के रूप में डाटा को नुकसान पहुंचाने वाली घटनाएं बहुत कम सामने आती हैं परन्तु इसका फिजीकल ड्राइव पर विनाशकारी प्रभाव पड़ सकता है । उदाहरणार्थ आग लगने, बाढ़ के कारण पानी से और प्लेटर में खरोंच पड़ने या प्लेटर के टूटने या दबाव में आने से ड्राईव प्रयोग के योग्य नहीं रह जाता । डाटा नुकसान को प्राकृतिक आपदा से बचाने का सर्वोत्तम उपाय है आफ साईट बैकअप (डाटा को अन्यत्र स्थान पर सुरक्षित रखना) । आपदा के आगमन का अनुमान संभव नहीं है, इसलिए सिस्टम बैकअप की एक प्रति आन–साईट तथा आफ–साईट पर होनी चाहिए । बैकअप का माध्यम सिस्टम, सॉफ्टवेयर तथा बैकअप की आवश्यक फ्रिकवेंसी पर निर्भर करेगा । यह भी सुनिश्चित करें कि बैक अप अनिवार्य रूप से हो तथा उसमें सम्पूर्ण डाटा सुरक्षित होना चाहिए ।

वायरस:

वायरस संक्रमण प्रतिमास लगभग 200–300 न्यू ट्रोजन की गति से नुकसान पहुॅचाता है । इस समय लगभग 65135 खतरनाक या नुकसान पहुॅचाने वाले वायरस है (स्रोत एसएआरसी दिनांक 1 सितम्बर, 2003) इनकी संख्या लगातार बढ़ती जा रही है तथा सिस्टम का वायरस से संक्रमित होने का गंभीर खतरा उत्पन्न हो चुका है । ऐसे वायरस के खतरे से बचाव के कई उपाय हैं:–

..3..

- यूजर डाटा में हैंकर के प्रवेश को रोकने के लिए सिस्टम में फायरवाल की स्थापना ।
- सिस्टम में एंटीवायरस प्रोग्राम स्थापित करें तथा स्केनिंग के लिए नियमित रूप से प्रयोग करें तथा सिस्टम यदि संक्रमित हो गया हो तो वायरस को हटाएं । कई वायरस निष्क्रिय रहते हैं या कई छोटे–छोटे परिवर्तन करते रहते हैं और धीरे–धीरे सिस्टम प्रणाली को खराब कर देते हैं । सुनिश्चित करें कि नियमित रूप से नये–नये एंटीवायरस प्रोग्राम का आवश्यकतानुसार प्रयोग किया जा रहा है ।
- बैक अप करें तथा बैकअप का संक्रमण देखने के लिए भी परीक्षण करें । वायरस संक्रमित बैक अप का प्रयोग करने का कोई लाभ नहीं है ।
- अपरिचित प्रेषक द्वारा भेजे गए अथवा यह मालूम न होने पर कि कहां से आया है और इसमें क्या है, ऐसे ई–मेल एटेचमेंट खोलने में सावधान रहें, इसे खोले नहीं केवल डिलीट करें तथा भविष्य की ई–मेल के लिए ऐसे प्रेषक को ब्लाक कर दें ।

त्रुटिया

उच्च प्रशिक्षित, प्रमाणित कम्प्यूटर ज्ञान प्राप्त कर्मचारियों के इस युग में भी अचानक होने वाली अनेक दुर्घटनाओं की हमेशा संभावना बनी रहती है । बचाव के लिए निम्नलिखित बातों का विशेष ध्यान रखेंः–

- सावधान रहें, यह कहना जितना आसान है व्यवहार में लाना उतना ही कठिन । डाटा को ट्रांसफर करते समय सुनिश्चित करें कि वह वांछित स्थान पर पहुॅच रहा है । यदि पूछा जाए would you like to replace the existing file तो yes को क्लिक करने से पहले पूरी सावधानी बरतें ।
- किसी कार्य के पूरा होने में संदेह रहने पर ध्यान रखें कि दुबारा प्रयोग करने के लिए उस डाटा की एक प्रति आपके पास है ।
- किसी ऐसे सॉफ्टवेयर जो ड्राइव डाटा स्टोरेज जैसे पार्टिशन मर्जर, फॉरमेट चेंज, डिस्क चेकर में परिवर्तन कर सकता है, के प्रयोग में अतिरिक्त सावधानी बरतें ।

..4..

- यदि नये ऑपरेटिंग सिस्टम को अपग्रेड करने में कोई समस्या आती है तो अपग्रेड करने से पहले अत्याधिक महत्वपूर्ण फाइलों और डायरेक्ट्रीयों का बैक अप ले लें । ध्यान रखें कि अलग–अलग डाटा ड्राईव को भी फार्मिट किया जा सकता है ।
- प्रोग्राम प्रयोग के समय कभी भी सिस्टम को बन्द न करें । खुली हुई फाईल इससे निष्क्रिय तथा बेकार हो सकती है ।

सॉफ्टवेयर खराबी

कम्प्यूटर का प्रयोग करते समय सॉफ्टवेयर की खराबी अवश्य ही सामने आती है । दुनिया के अच्छे से अच्छे प्रोग्राम में भी उसमें आने वाली प्रत्येक खराबी का पूर्व अनुमान सम्भव नहीं है । कुछ बातों का ध्यान रखते हुए इसके नुकसान को कम किया जा सकता है ।

- सुनिश्चित करें कि सॉफ्टवेयर केवल इसके निर्धारित उद्देश्य के लिए प्रयोग किया जा रहा है । प्रोग्राम का दुरूपयोग से इसमें खराबी आ सकती है ।
- प्रोग्राम की नकली (पायरेटिड) प्रति प्रयोग करने से भी सॉफ्टवेयर में खराबी के परिणामस्वरूप डाटा फाईलों में खराबी आ सकती है ।
- सुनिश्चित करें कि एक समय में अनेक प्रोग्रामों में कार्य करते समय यथावश्यक मैमोरी क्षमता स्थापित की गई है । यदि प्रोग्राम बन्द या हैंग हो जाता है तो डाटा समाप्त या भ्रष्ट हो सकता है ।
- यद्यपि बैक अप कठिन कार्य है परन्तु यह सॉफ्टवेयर में खराबी आने पर बहुत उपयोगी सिद्ध होता है ।

हॉर्डवेयर खराबी

डाटा नुकसान हार्डवेयर खराबी या हार्डड्राईव में खराबी ऐसी आम समस्याएं हैं जो कम्प्यूटिंग में अवश्य रूप में सामने आती हैं । प्रायः ऐसी कोई विधि नहीं हैं कि जो हार्डड्राईव के फेल होने की चेतावनी दे । परन्तु इस प्रकार के नुकसान से बचाव के लिए कुछ उपाय किए जा सकते हैं:–

- स्टेक ड्राईव को एक दूसरे के उपर न रखें तथा वायु संचार के लिये उचित स्थान छोड़ें अत्याधिक गर्मी से ड्राईव खराब हो जाती है । सुनिश्चित करें कि कम्प्यूटर को गर्मी पैदा करने वाले उपकरणों से दूर रखें तथा वायु संचार की अच्छी व्यवस्था हो ।
- हमेशा यूपीएस का प्रयोग करें ताकि बिजली की गड़बड़ी से होने वाली खराबियों से बचा जा सके ।
- हार्डड्राईव के उपर वाले स्थान पर सामान न रखें । ड्राईव के भीतर प्लेटर पर धूल का कण जाने से यह खराब हो सकता है ।
- यदि सिस्टम प्रत्येक रीबूट पर स्केनडिस्क का प्रयोग करता है तो इससे पता चलता है कि सिस्टम में डाटा में नुकसान होने का खतरा है । शीघ्र ही इसका बैक अप कर लें ।
- यदि सिस्टम में ड्राईव से कोई असामान्य आवाज आती है तो सिस्टम को बन्द करके हार्डवेयर इंजीनियर से इसका कारण जाने ।

1.3 वायरस

वायरस एक प्रकार का नुकसानदायक कोड हे जो भारी हानि पहुॅचा सकता है, इसे गुप्त रूप से भी एक कम्प्यूटर से दूसरे कम्प्यूटर में पहुंचाया जा सकता है । । वायरस शब्द में इसके सभी बड़े वायरसों सहित ट्रोजन्स तथा वार्मस आदि वायरस आते हैं । परन्तु सुविधा के लिए इन सभी प्रोग्रामों को केवल वायरस कहा गया है । वायरसों को तीन श्रेणियों में रखा जा सकता है :–

खतरनाक:– जैसे रिज्यूम और लव लैटर जो कभी–कभी कम्प्यूटर सिस्टम फाईलों तथा कम्प्यूटर के भण्डारण साधनों में रखे गये प्रोग्रामों और डाटा को अपूर्णीय क्षति पहुंचाते हैं । साथ ही यूजर आईडी तथा पासवर्ड सूचना को चुराने का भी प्रयास करते हैं ।
बचकाना:– येके,हिचकॉक,फिल्प और डायमंड जैसे वायरस सामान्यतः डेटा, प्रोग्रामों या बूट रिकार्ड को खराब या नष्ट नहीं कर पाते परन्तु बचकाने एवं भद्दे संदेश, संगीत, स्कीन पर झटके देना या ऐनीमेट रेखा चित्रों को दिखाना जैसे कार्यों से बाधा पहुंचाता है ।

अप्रभावी :–बल्ह जैसे वायरस वैसे तो कुछ नहीं करते परंतु बार–बार सामने आते हैं या सिस्टम में फाइलों के साथ जुड़ जाते है जिससे स्टोरेज मीडिया में रूकावट पैदा होने लगती है । इनमें से अधिकांश वायरस खराब लिखित कोड के कारण अप्रभावी रहते हैं – इनका कुछ न कुछ प्रभाव तो पड़ता ही है परंतु वायरस राइटर इसे सही प्रकार से पहचान नहीं पाता ।
इन सभी वायरसों के भीतर ही कुछ ऐसे वायरस भी हैं जो प्रायः 'विशेष स्थिति' में क्रियाशील होते हैं जैसे कोई तारीख 1 अप्रेल अथवा 31 अक्टूबर अथवा प्रतिदिन 15.10 बजने पर जब चाय के समय (Tea Time) वाले वायरस किग्राशील होते हैं ।

वायरस संक्रमण से कम्प्यूटर का बचाव

- महत्वपूर्ण डाटा का नियमित बैकअप लेना।
- कम्प्यूटर में एंटीवायरस सॉफ्टवेयर की स्थापना और उसका दैनिक उपयोग करना ।
- नवीनतम सिगनेचर फाइलों वाले एंटीवायरस को साप्ताहिक/पाक्षिक रूप से संशोधित (अपडेट) करना । यदि एंटीवायरस सॉफ्टवेयर को नए–नए वायरसों के अनुसार संशोधित नहीं किया जाता तो यह बहुत प्रभावी नहीं होते ।
- एंटीवायरस साफटवेयर को नवीनतम संस्करण के अनुसार अपग्रेड करना ।

अपरिचित स्रोत से प्राप्त फाइल अथवा संलग्नक वाले ई–मेल को न खोले और न ही ऐसी फाइल को प्रयोग करें । यदि यूजर को स्रोत की पूरी जानकारी नहीं है तो इसे मिटा दे । कुछ वायरस इस प्रकार लिखे जाते हैं कि ऐसा प्रतीत हो कि वह मित्र या किसी सहयोगी से प्राप्त हुए हैं । अतः विश्वसनीय स्रोत से प्राप्त संलनग्क वाले इ मेल भी खोलते समय सावधानी बरते क्योंकि ऐसे संलग्नक में अज्ञानतावश भेजे गए वायरस हो सकते है । ऐसी स्थिति में इसे फाइल में सुरक्षित (save) कर वायरेस स्केन सॉफ्टवेयर का उपयोग करने से वायरस को समाप्त किया जा सकता है ।

2. जरनल यूजर संबंधित नीतियां

2.1 सीडी/फलेश ड्राइवस/फलापियों का उपयोग

- फलापियों का उपयोग सिस्टम एडमिनिस्ट्रेटर /इंचार्ज कम्प्यूटर सेंटर की सलाह से किया जाना चाहिए तथा उपयोग से पहले एंटीवायरस सॉफ्टवेयर की मदद से इसे टेस्ट कर लिया जाना कर लेनी चाहिए ।
- आफिस सिस्टमों में अन–ऑफिशयल/पायरेटिड सीडी/फलेश ड्राइवस/फलापियों का उपयोग नहीं किया जाना चाहिए ।
- फलापी से सिस्टम में डेटा ट्रांसफर करने के लिए फलापी राइट–प्रोटेक्टेड मोड होनी चाहिए ।

2.2 पासवर्ड

- सिस्टम स्क्रीन सेवर पासवर्ड इनेबिल करके रखा जाना चाहिए ।
- पासवर्ड गुप्त रखें और किसी को भी न बतायें ।
- नेटवर्क एक्सेस, सक्रीन सेवर इत्यादि के पासवर्ड बनाते समय हमेशा यह ध्यान में रखें कि वे इतने सरल न हों कि अन्य कोई आसानी से इनका पता लगा सके ।
- बड़े–छोटे अक्षर, संख्या और विरामचिन्ह को मिला कर जितना संभव हो बड़ा और सुरक्षित पासवर्ड बनाया जाना चाहिए और किसी व्यक्तिगत सूचना, अथवा किसी भाषा के अक्षर पर आधारित नहीं होना चाहिए ।
- एक जैसा पासवर्ड दोबारा न बनाएं ।
- समय–समय पर पासवर्ड बदलते रहें ।

2.3 बैकअप

- विभागीय नीति के अनुसार विभाग के सेंट्रल सरवर में निर्धारित स्थान पर अथवा स्टोरेज मीडिया में नियमित रूप से बैकअप को लेना चाहिए ।
- सरवर की कन्फिग्रेशन फाइल का प्रिंट आउट किसी सुरक्षित जगह रखा जाना चाहिए ।

- टेप अथवा दूसरे रिमूवबल मीडिया को कम्प्यूटर रूम के बाहर सुरक्षित स्थान में रखा जाना चाहिए ।
- वर्कस्टेशन छोड़ने से पहले बैकअप अवश्य लिया जाना चाहिए ।
- सेंसटिव और महत्वपूर्ण डाटा के लिए आफ साइट बैकअप का उपयोग किया जाना चाहिए ।

2.4 सिस्टम की सुरक्षा

- सिस्टम के अनधिकार उपयोग और किसी प्रकार की हानि से बचाव हेतु कार्यालय छोड़ते समय सुरक्षा व्यवस्था के लिए तालाबंद किया जाना चाहिए ।
- पोर्टेबल उपकरणों को सुरक्षित स्थान पर रखना चाहिए ।
- मॉनिटर और प्रिंटरों को इस प्रकार से रखें कि अन्य कोई सेन्सिटिव डाटा न देख सके ।
- फलापी डिस्कस और दूसरे मीडिया को सुरक्षित स्थान में रखें।
- उपकरणों के निपटान (राइट आफ) से पहले किसी विशेषज्ञ की सहायता लेनी चाहिए ।
- डाटा अथवा उपसाधन के किसी प्रकार के नुकसान के बारे में सिस्टम एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर को रिपोर्ट की जानी चाहिए।
- बाहरी लोगों से सिस्टम और सेंसटिव डाटा का बचाव करें ।
- उपकरण बाहर ले जाने से पूर्व आवश्यक अनुमति प्राप्त करें ।
- उपकरण उठाते समय भी विशेष सावधानी बरतें । (इसके लिए उपकरण पर लिखे अनुदेश देखें)
- विद्युत आपूर्ति बाधा से डाटा में होने वाली हानि के बचाव के लिए समुचित बैटरी बैकअप वाले यूपीएस सिस्टम की स्थापना करें ।
- कार्यालय छोड़ने से पहले सिस्टम को अच्छी तरह से बंद करें ।
- सीट छोड़ते समय भी सिस्टम को लागऑफ करें ।
- कम्प्यूटर ऑन होने की स्थिति में केबल न निकालें इससे बिजली का शाट–सर्किट हो सकता है ।
- सिस्टम के अच्छी तरह शुरू होने तक स्केनडिस्क को न रोकें ।
- हमेशा माउसपेड पर ही माउस का उपयोग करें ।
- कीबोर्ड और माउस का उचित उपयोग करें ।
- हार्डवेयर को खुला न छोड़ें ।
- ध्यान रखें कि सिस्टम से जुड़ी केबल अधिक कसी हुई न हों ।

2.5 कम्प्यूटर फाइलें

- समस्त फाइल स्तर की सुरक्षा फाइल सिस्टम पर ही निर्भर करती है । सर्वर के लिए सबसे उपयुक्त फाइल संरक्षण सिस्टम का चुनाव किया जाना चाहिए । तदनुसार व्यक्तिगत फाइलों, फोल्डर्स, ड्राइव एक्सेस की अनुमति दी जानी चाहिए ।
- किसी भी प्रकार की अनुचित भागीदारी (डिफाल्ट शेयरिंग) को समाप्त किया जाना चाहिए ।
- केवल वांछित फाइल और आब्जेकट सर्वर पर उपलब्ध कराये जाने चाहिए ।
- अपरिचित इमेल आइडी के माध्यम से प्राप्त एटेच्ड फाइल को खोलने अथवा डाउनलोड करने से बचा जाना चाहिए ।
- कम्प्यूटर में फाइलें सुव्यवस्थित ढंग से रखें जिससे वह आसानी से उपलब्ध हो सके । आवश्यकतानुसार नए फोलडर अथवा सबफोलडर बनाए जाने चाहिए ।
- अत्याधिक फाइल और फोल्डर बनाने से बचा जाना चाहिए।
- सिस्टम फाइलों और लाइयब्रेरी को एक्सेसड न करें इससे आपरेटिंग सिस्टम के खराब होने का डर रहता है ।
- डाटा को ट्रांसफर करते समय सुनिश्चित करें कि वह वांछित स्थान पर पहुॅच रहा है । यदि पूछा जाए would you like to replace the existing file तो yes को क्लिक करने से पहले पूरी सावधानी बरतें ।

2.6 सामान्य अनुदेश

- किसी कार्य के पूरा होने में संदेह रहने पर ध्यान रखें कि दुबारा प्रयोग करने के लिए उस डाटा की एक प्रति आपके पास है ।
- सिस्टम एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर द्वारा पद्धति के बारे में समय–समय पर जारी अनुदेशों का भली–भांति पालन किया जाना चाहिए ।
- कम्प्यूटरों पर व्यक्तिगत कार्य नहीं किया जाना चाहिए ।
- सिस्टम खराब होने की स्थिति में सिस्टम एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर को सूचित किया जाना चाहिए।
- हमेशा अपनी मशीन पर ही काम किया जाना चाहिए तथा विशेष परिस्थितियों में सिस्टम एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर की अनुमति से ही दूसरी मशीन का उपयोग होना चाहिए ।

- सिस्टम एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर की सलाह से समय–समय पर एंटीवायरस साफटवेयर को अपडेटिड किया जाना चाहिए ।
- कार्य करते समय बाहरी लोगों से सेंसटिव डाटा/महत्वपूर्ण विषयवस्तु का बचाव किया जाना चाहिए ।
- शेयरवेयर सॉफटवेयर का बहुत अधिक प्रयोग नहीं करना चाहिए ।
- एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर की अनुमति के बिना सिस्टम पर किसी साफटवेयर की स्थापना नहीं की जानी चाहिए ।
- इंटरनेट के अनावश्यक उपयोग से बचा जाना चाहिए ।
- सिस्टम हैंग होने पर घबराना नहीं चाहिए । इसकी सूचना तुरंत अपने नोडल आफिसर/सिस्टम एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर को दी जानी चाहिए ।
- सुरक्षा व्यवस्था के लिए ताला बंद व्यवस्था के साथ ही यूजर को भी कम्प्यूटर के सभी उपकरणों की पूरी देखभाल रखनी चाहिए ।
- सिस्टम में पूर्व स्थापित एंटीवायरस ठीक से काम करने पर ध्यान दिया जाना चाहिए ।
- सिस्टम के पास खाने पीने की चीजें नहीं रखी जानी चाहिए । सीपीयू, मॉनिटर और कीबोर्ड के पास चाय/काफी के कप और पानी का गिलास नहीं रखे जाने चाहिए ।
- सिस्टम की सफाई करते समय विद्युत स्विच बन्द रखना चाहिए ।
- स्क्रीन को साफ करते समय गीले कपड़े का उपयोग नहीं किया जाना चाहिए।
- किसी प्रोग्राम पर कार्य करते समय सिस्टम को सीधे ही बंद नहीं किया जाना चाहिए । इससे खुली हुई फाइलें भ्रष्ट–नष्ट हो जाती हैं ।
- सीपीयू पर फाइलें, किताबें इत्यादि किसी प्रकार की सामग्री नहीं रखी जानी चाहिए ।
- कार्य समाप्ति पर कम्प्यूटर को ढक कर रखा जाना चाहिए ।

3 विभागीय नीति

- प्रत्येक विभाग में सिस्टम एडमिनिस्ट्रेटर/इंचार्ज कम्प्यूटर सेंटर अवश्य होना चाहिए ।
- विभाग के कर्मचारियों को दिल्ली सरकार की सुरक्षा नीतियों की पूरी जानकारी होनी चाहिए ।
- प्रत्येक विभाग में आवश्यकतानुसार लिखित सुरक्षा नीतिया, मानकों और प्रक्रियाओं का प्रावधान होना चाहिए ।

- प्रशासक के लिए स्पष्ट परिभाषित सिस्टम सुरक्षा प्रणालियां होनी चाहिए ।
- आईटी सुरक्षा संबंधित दायित्व एवं नीतियों के कुशलतापूर्वक निवर्हन के लिए विभाग के कर्मचारियेां को आवश्यक प्राधिकार दिए जाने चाहिए ।
- नियमित प्रशासक की अनुपस्थिति में आईटी सुरक्षा संबंधित दायित्वों के निवर्हन के लिए सक्षम कर्मचारी को प्राधिकार दिए जाने चाहिए ।
- विभाग में किसी हानि अथवा समस्या के समाधान के लिए निर्धारित प्रकिया होनी चाहिए ।
- कम्प्यूटर उपकरणों को संभावित खतरों से बचाने के लिए इन्हें सुरक्षित ढंग से रखने की व्यवस्था होनी चाहिए । जैसे छत का टपकना इत्यादि ।
- सर्वरों और वर्कस्टेशनों के लिए बिना बाधित विद्युत आपूर्ति व्यवस्था (यूपीएस)की व्यवस्था होनी चाहिए ।
- कम्प्यूटर कक्ष में उचित तापमान की व्यवस्था होनी चाहिए ।
- विभाग में कड़े पासवर्डों वाले सॉफ्टवेयर का ही उपयोग किया जाना चाहिए ।
- भूल गये पासवर्डों के लिए लिखित पद्धति होनी चाहिए ।
- व्यवहारिक सुरक्षा की जांच–पड़ताल करते रहना चाहिए ।
- विभाग में व्यवहारिक सुरक्षा मानकों एवं प्रणालियां का प्रावधान होना चाहिए ।
- आईटी कक्षों ,टेलीफोन और कम्प्यूटर्स कक्षों की तालाबंद सुरक्षा व्यवस्था प्रणाली होनी चाहिए ।
- विभाग में अलार्म सिस्टम होना चाहिए ।
- कार्यालय/विभाग में छुट्टी के समय सिस्टम के किसी भी प्रकार के अनुचित उपयोग को रोकने के लिए पक्की सुरक्षा व्यवस्था होनी चाहिए ।
- वर्कस्टेशनों और लैपटाप की चोरी रोकने के लिए तालाबंद सुरक्षा व्यवस्था होनी चाहिए ।
- विभाग में नेटवर्क /लेन (लोकल एरिया नेटवर्क) के मेप/डायाग्राम होने चाहिए ।
- विक्रेताओं से भागीदारी होनी चाहिए जिससे वे सिस्टम में नुकसान की संकटकालीन स्थिति में मदद कर सकें ।
- बैकअप फाइलों को अन्यत्र सुरक्षित स्थानों पर रखने की व्यवस्था होनी चाहिए ।

- आफसाइट मीडिया स्टोर में तापमान व्यवस्था (तापमान नमी इत्यादि) बैकअप मीडिया उत्पादकों के निर्देशानुसार ही होना चाहिए ।
- विभाग में सभी हार्डवेयर और साफटवेयर उत्पादों की कन्फिग्रेशन/ऐसट कंट्रोल प्लान होनी चाहिए
- कम्प्यूटर और साफटवेयर उपकरणों की स्थापना के लिए केवल प्रशिक्षित लोगों को प्राधिकार दिए जाने चाहिए ।