सुरक्षित पासवर्ड सम्बन्धी अभ्यासहरु

प्रमाणीकरण नियन्त्रकको कार्यालय

विज्ञान तथा प्रविधि मन्त्रालय

सिंहदरवार काठमाण्डौ

१. परिचय

१.१. सुरक्षित पासवर्ड सम्वन्धी अभ्यासहरु पासवर्डको निर्माण र प्रयोगको सन्दर्भमा प्रचलित नियमहरुको संग्रह हो । यो अभ्यासहरुको संग्रह कम्प्यूटर प्रणालीको सुरक्षालाई बढावा दिन बलियो पासवर्ड निर्माण गरी तिनको उपयोग गर्न नेपाल सरकारका विभिन्न संगठनहरुमा कार्यरत कर्मचारीहरुलाई अभिप्रेरित गर्न तयार गरिएको हो । यो सामान्यतः हरेक कर्यालयहरुको कार्यालय सम्वन्धी दैनिक नियमहरुको एक अभिन्न पाटो हुन सक्दछ । यसलाई सुरक्षा सचेतना तालिमको प्रशिक्षणको विषय पनि बनाउन सकिन्छ । यसलाई बाध्यकारी वा सुझावमूलक साधनको रुपमा सरकारी संगठनहरुले प्रयोग गर्न सक्दछन् ।

२. विषय प्रवेश

२.१. पासवर्ड कम्प्यूटर र सूचना सुरक्षणको एक महत्वपूर्ण अवधारणा हो । पासवर्डले कम्प्यूटर प्रयोगकर्ताहरुको एकाउन्टको अग्रभागमा रहेर सुरक्षा प्रदान गर्दछ । कमजोर पासवर्डको प्रयोगले संगठनको समग्र संस्थागत संजाल (Corporate Network) को सूचनाको विश्वसनीयता कायम राख्न सकिदैन । यसैले प्रत्येक कर्मचारी, करार सेवा प्रदायकहरु, विक्रेताहरु तगायतका कार्यालयका सूचना प्रणालीसँग सरोकार र सम्वन्ध हुने हरेक व्यक्तिले सुरक्षित पासवर्ड तयार गर्न र यस अभ्यासहरुमा उल्लेख भएका विषयहरु र त्यसका चरणहरुको अनुसरण गर्नु राम्रो हुन्छ ।

२.२. संगठनको सूचना प्रणालीसँग सम्वद्ध कर्मचारीले त आफ्नो संगठनको सूचना सञ्जाल, तथ्याङ्कको विश्वसनीयता र कम्प्यूटर प्रणालीको सुरक्षा गर्न यी अभ्यासहरुलाई पालना गर्नु अनिवार्य नै हुने देखिन्छ ।

३. उद्देश्यहरु

३.१. यस निर्देशिकाको मूलभूत उद्देश्य संगठनको सूचना, त्यसको स्रोत र सूचना तथा कम्प्यूटर सञ्जालको सुरक्षाका लागि बलियो पासवर्डको सिर्जना, पासवर्डहरुको सुरक्षा तथा समय समयमा परिवर्तन गर्न स्तरीय मानदण्डहरुको निर्धारण गर्नु नै हो । संगठनको सूचना प्रणाली पासवर्डको प्रयोग मात्रले शतप्रतिशत सुरक्षा गर्न नसकिए पनि डिजिटल हस्ताक्षर जारी नभए सम्मका लागि यो नै बढी भरपर्दो प्रविधि भने हो भन्न सकिन्छ । यी अभ्यासहरुले पासवर्डको प्रयोगलाई बढी विश्वसनीय बनाउन सहयोग गर्दछन् ।

४. क्षेत्र

४.१. यी अभ्यासहरु कार्यालयको सूचना प्रणालीमा कार्यालयको तर्फबाट व्यक्तिगत वा सांगठनिक एकाउन्टको सुविधा प्राप्त गरेका, संगठनको कम्प्यूटर सञ्जाल, सूचना प्रणाली तथा सबै प्रकारको सूचना भण्डारमा पहुँच भएका वा सो को जिम्मेवारी भएका सबै कर्मचारीहरुलाई लक्षित गरी तयार गरिएका हुन् । तर यो डोमेन एकाउन्ट वा इमेल एकाउन्टमा मात्र सीमित भने छैन ।

५. पासवर्ड सम्वन्धी प्रचलित अभ्यासहरु

५.१. पासवर्ड सुरक्षा सम्वन्धी साधारण अभ्यासहरु

५.१.१. सबै सिस्टम लेभलमा प्रयोग हुने पासवर्डहरु (जस्तोः Root, NT Admin, Application Administration Account आदि) कम्तिमा पनि त्रैमासिक रुपमा परिवर्तन गरिरहनु पर्दछ ।

५.१.२. सबै प्रोडक्सन लेभलमा प्रयोग गरिएका पासवर्डहरुले ग्लोवल पासवर्ड व्यवस्थापन डाटावेशद्वारा निर्देशित सूचना सुरक्षणको अनुसरण गरेको हुनु पर्दछ ।

५.१.३. सबै यूजर लेभलका पासवर्डहरु जस्तोः इमेल, वेव, डेस्कटप कम्प्यूटर आदि कम्तिमा पनि द्वैमासिक रुपमा अनिवार्य परिवर्तन गरिरहनु पर्दछ । यद्यपी हरेक महिनामा परिवर्तन गर्न सके अझ बढी भरपर्दो र सुरक्षित हुन सक्दछ ।

५.१.४. समूह सदस्यता वा कार्यक्रमको सिस्टम लेभलको विशेष सुविधाबाट प्राप्त यूजर एकाउन्टहरुको प्रयोगकर्ताहरुले प्रयोग गर्ने पासवर्ड अन्य सबै एकाउन्टहरुको भन्दा भिन्न प्रकृतिको हुनु पर्दछ ।

५.१.५. एकाउन्ट लकआउट थ्रेसहोल्ड चार पटकको गलत पासवर्ड प्रयासमा निर्धारण गरिनु राम्रो हुन्छ । यसको अर्थ लगातार चारपटकसम्मा गलत पासवर्ड इन्ट्री गरेमा एकाउन्ट लक हुने व्यवस्था गर्नु उपयुक्त हुन्छ ।

५.१.६. एसएनएमपी (साधारण नेटवर्क व्यवस्थापन प्रोटोकल) प्रयोग गरिएको भए सो को कम्यूनिटी स्ट्रीङ पब्लिक, प्राईभेट र सिस्टमको स्टेन्डर्ड डिफल्ट भन्दा भिन्न हुने गरी प्रयोग हुनु पर्दछ । साथै बारम्बार लगईन गर्न प्रयोग गरिने पासवर्ड भन्दा भिन्न हुनु पर्दछ । यसका लागि सम्भव भए सम्म कीड ह्यास (Keyed Hash) प्रयोग गरिनु उपयुक्त हुन्छ ।

५.१.७. सबै प्रकारका सिस्टम लेभल र युजर लेभलका पासवर्डहरु यी अभ्यासहरुमा उल्लेखित विषयहरुको अनुरुप हुने गरी तयार गर्नु पर्दछ ।

५.१.८. विगतमा प्रयोग गरिएका पासवर्डहरु पुनः प्रयोग गर्न सकिन्छ । तर निश्चित संख्याका नयाँ पासवर्डहरु प्रयोग नगरी पुरानो पासवर्ड प्रयोग नगर्नु राम्रो हुन्छ । यसका लागि कम्तिमा पनि चौवीस वटा नयाँ पासवर्डको प्रयोग पछि मात्र पुरानो पासवर्ड दोहोऱ्याउनु उपयुक्त हुन्छ ।

५.१.९. गलत पासवर्ड प्रयोग भएको भन्ने आधारको गणना गर्ने समयावधी निर्धारण गर्दा समान्यतः बीस मिनेट भित्रको अन्तरालमा कायम गरिनु राम्रो हुन्छ । यसको अर्थ यदि बीस मिनेटभित्रको अन्तरालमा तीन पटकसम्म प्रयास गरिएमा एकाउन्ट लकआउट हुने व्यवस्था गर्नु पर्दछ ।

५.१.१०. एकाउन्ट लकआउट हुने अवधिका लागि विज्ञहरुले कम्तिमा बिस मिनेट र बढीमा दुई घण्टा निर्धारण गर्नु उपयुक्त हुने धारणा राखेका छन् ।

५.१.११. कम्प्यूटरको सुरक्षाका लागि पासवर्डद्वारा सुरक्षित स्क्रिन सेभर इनेवल गर्नु पर्दछ । सामान्यतः कम्प्यूटर प्रयोगकर्ताले पाँच मिनेट समयसम्म लगातार निष्कृय रहेमा यस्तो हुने व्यवस्था गर्नु पर्दछ । युजर लगअन भइरहेको अवस्थामा वा पासवर्ड सुरक्षित स्क्रिन सेभर प्रयोग नभएको अवस्थामा कम्प्यूटर छोड्नै हुदैन । कम्प्यूटर लक नगरिएको अवस्थामा नै छोडेर हिड्ने बानी सबैले सुधार गनै पर्दछ । हतार भएको अवस्थामा CTRL+ALT+DEL अथवा Windows Key+L को प्रयोग गरी सिधै लकआउट गर्न सकिन्छ ।

५.१.१२. पव्लिक प्राइभेट साँचोको आधिकारिकताका लागि प्रयोग हुने पासफ्रेजहरुका लागि समेत पासवर्डका लागि निर्धारित नियमहरु अक्षरश लागु हुन्छन् ।

५.१.१३. Eudora, Outlook, Netscape, Mozila Firefox, Internet Explorer लगायतका ब्राउजरहरु जस्ता एप्लिकेशनहरुमा हुने पासवर्ड सम्झने (Remember password) सुविधा प्रयोग नगर्नु नै राम्रो मानिन्छ ।

५.१.१४. पासवर्ड प्रयोग गरेर आफ्नो संगठनको सूचना प्रणालीमा पहुँच पुग्ने कार्य साईवर क्याफे जस्ता सार्वजनिक नेटवर्कहरुबाट गर्नु हुदैन ।

५.२. पासवर्ड निर्माणका मार्गदर्शक निर्देशनहरु

५.२.१. कार्यालय वा संगठनमा धेरै उद्देश्यका लागि पासवर्डहरु प्रयोग गरिन्छ । सामान्यतयाः युजर लेभलका एकाउन्टहरु, वेव एकाउन्टहरु, ईमेल एकाउन्टहरु, स्क्रिन सेभर सुरक्षा, भ्वाईसमेल तथा लोकल राउटर लगईनहरुमा धेरैजसो सबैले पासवर्डहरु प्रयोग गर्ने गर्दछन् । अत्यन्त कम सिस्टमहरुमा मात्र एकपटकको टोकन विधि (एकपटकमात्र प्रयोग गरिने गतिशील पासवर्डहरु) को प्रयोग गरिन्छ । सबै

सिस्टममा यो विधि सम्भव पनि छैन । त्यसैले पनि बारम्बार प्रयोग गरिने पासवर्ड बलियो बनाउन, छनौट गर्न तथा सुरक्षित रुपमा प्रयोग गर्न सधै सतर्क रहनु पर्दछ । देहायका अवस्थाहरु रहेका पासवर्डहरु सामान्यत कमजोर ठानिन्छन् ।

५.२.१.१. आठ क्यारेक्टर भन्दा थोरै संख्या भएका पासवर्डहरु,

५.२.१.२. अंग्रेजी वा अन्य भाषाका शब्दकोषमा पाईने शब्दहरु,

५.२.१.३. समान्यतः प्रयोगमा आईरहने शब्दहरु जस्तोः

५.२.१.३.१. परिवार, घरपालुवा जनावर, साथीहरु, सहकर्मीहरु,

५.२.१.३.२. कम्प्यूटरमा प्रयोग गरिने पदावली नामहरु, कमान्डहरु, साईटहरु, कम्पनीहरु, हार्डवेयर, सफ्टवेयर आदि ।

५.२.१.३.३. कम्पनी वा संगठनको नाम, स्थान विशेषको नाम अथवा अन्य KTM, BRT, वा अन्य त्यस्तै डेरिभेटिभ शब्दहरु,

५.२.१.३.४. जन्ममिति, टेलिफोन नम्वर, परिचयपत्र नम्वर, ठेगाना जस्ता व्यक्तिगत सूचनाहरु,

५.२.१.३.५. कम्प्यूटरको कीवोर्ड वा प्रचलित वर्णमालाका अक्षर वा अंकहरुको क्रम, जस्तोः aaabbb, qwerty, 12345, zyxwvuts, 456654 आदि,

५.२.१.३.६. माथिका बुँदाहरुमा उल्लेख गरिएका कुनै पनि शब्दहरुको पछाडि पट्टिबाछ हिज्जे मिलाईएका शब्दहरु

५.२.१.३.७. माथि उल्लेख गरिएका कुनै पनि शब्दहरुको अगाडि वा पछाडि अंक जोडेर बनाईएका शब्दहरु जस्तो DoLIDAR1, 3MoGA, OCC123 आदि ।

५.२.२. बलियो पासवर्डका देहाय अनुसारका विशेषताहरु हुन्छन् ।

५.२.२.१. वर्णमालाका ठूला तथा साना अक्षर मिसाईएका शब्दहरु (जस्तो, a-z, A-Z),

५.२.२.२. अक्षर, अङ्क तथा विराम चिन्हहरु मिसाईएर प्रयोग गरिएका शब्दहरु (जस्तो, 0-9, *{%$#_,

५.२.२.३. न्यूनतम आठवटा अक्षरअङ्क प्रयोग भएके र सम्भवतः पासफ्रेज हुने गरी,

५.२.२.४. कुनै पनि भाषा, भाषिका, बोलीचालीको भाषा अथवा जार्गनहरु प्रयोग नभएको शब्द,

५.२.२.५. व्यक्तिगत सूचना, नामहरु तथा पारिवारिक विवरण प्रयोग नगरिएका शब्दहरु,

५.२.२.६. पासवर्डहरु कहिँ कतै अनलाईनमा लेख्न वा संग्रह गरेर राख्नु हुदैन । यथासम्भव सजिलै सम्झन सकिने पासवर्डहरु तयार गर्नु पर्दछ । यसको लागि एउटा उत्तम उपायको रुपमा कुनै गीतको शिर्षक, आफूसँग सम्वन्ध राख्ने

विषयहरु अथवा यस्तै प्रकारको अन्य कुनै फ्रेजहरु हुन वाक्य वा वाक्यांशहरु हुन सक्दछ । उदाहरणको लागि एउटा वाक्य 'This may be one way to remember" र यसबाट बनेको पासवर्ड "TmB1w2r" अथवा "tmb1w-r" अथवा अन्य कुनै यस्तै प्रकारको अलग रुपमा तयार गरिएको हुन सक्दछ । यसमा हरेक शब्दको पहिलो अक्षर लिई संभव भएकालाई नम्वरमा परिणत गरी तयार गरिएको छ ।

५.२.२.७. पासवर्डहरु केश (वर्णमालाका साना तथा ठूला अक्षरहरु) सम्वेदनशील हुनु पर्दछ तर लगईन आईडी भने यस्तो नभए पनि हुन्छ ।

५.२.३. यस अभ्यासहरुमा उदाहरणको रुपमा प्रयोग गरिएका शब्द वा फ्रेजलाई पासवर्डको रुपमा प्रयोग गर्ने हुदैन ।

५.२.४. फ्रेज प्रयोग गरेर पासवर्ड निर्माण गर्ने तरिका:

५.२.४.१. शब्दहरु वा शब्दांशहरुलाई एक अर्कोसँग जोड्ने ।

५.२.४.२. पासवर्डको रुपमा प्रयोग गरिएको शब्द वा शब्दांशको हिज्जे गलत वनाउने,

५.२.४.३. बीच बीचमा एक वा दुई शब्दहरु छोड्ने ।

५.२.४.४. आफूसँग व्यक्तिगत सम्वन्ध भएका फ्रेजहरुलाई प्रयोग गरी उक्त फ्रेजको प्रत्येक शब्दको पहिलो, दोश्रो वा तेस्रो अक्षरको संयोजन गरी तयार गर्ने । यस्तो फ्रेज प्रश्न वा उत्तर कुनै पनि रुपमा प्रयोग गर्न सकिन्छ । यसका लागि तरिकाहरु धेरै हुन सक्दछन्, जस्तैः

५.२.४.४.१. अन्तिममा संख्या हुने पासफ्रेजहरु प्रयोग गर्ने,

५.२.४.४.२. पासवर्ड वनाईसकेपछि अंक र अक्षरलाई संझन सक्ने गरी यताउता सार्ने,

५.२.४.४.३. प्रश्न भन्दा अगाडि उत्तरको भाग प्रयोग गर्ने,

५.२.४.४.४. वर्णमालाको ठूलो अक्षर र साना अक्षरहरु मिश्रित रुपमा प्रयोग गर्ने । फ्रेजमा ठूलो अक्षर प्रयोग गर्दा असामान्य क्रममा प्रयोग गर्ने ।

५.२.४.४.५. फ्रेजमा कुनै भाग वा कुनै शब्दको लागि प्रयोग गरिएको अक्षरको सट्टा सम्भव भए अङ्क प्रयोग गर्ने ।

५.२.४.४.६. फ्रेजको कुनै भागमा विराम चिन्ह तथा अन्य कुनै विशेष चिन्हहरु प्रयोग गर्ने ।

५.२.५. केहि वलियो पासवर्डका उदाहरणहरु

५.२.५.१. तलका उदाहरणहरुमा विशेष चिन्हहरु अन्तमा वा शुरुमा प्रयोग गर्ने चलन उल्लेख भएपनि पनि पासवर्ड अझ प्रश्न उत्तर फ्रेजहरुले बनेको पासवर्डको हकमा बीच भागमा प्रयोग गर्न सकिएमा विराम चिन्हले पासवर्डलाई धेरै बलियो बनाउन सहयोग गर्दछ ।

५.२.५.१.१. अन्तमा अङ्क प्रयोग गरिएको फ्रेज, "My favorite number is 333" बाट पासवर्ड MFNI333 अथवा "Yaus333" बनाउन सकिन्छ । यसमा पहिलो र दोश्रो अक्षरको प्रयोग गरी पासवर्ड तयार गरिएको छ ।

५.२.५.१.२. प्रश्न तथा त्यसको उत्तरको फ्रेज प्रयोग गरिएको जसमा उत्तरको पहिलो अक्षरलाई अङ्कले सङ्केत गरिएको छ ।

My Favorite song is "Dust in the Wind", Password: "MFSI492023!"

५.२.५.१.३. प्रश्न तथा त्यसको उत्तरको फ्रेज प्रयोग गरिएको, जसमा उत्तरको सबै अक्षरलाई अङ्कले सङ्केत गरिएको छ ।

The name of my favorite grandchild is Tim. Password: "tnomfg!#20913"

The name of my favorite aunt is Lois. Password: "Tnomfai1215919"

My aunt's name is Lois. Password: "%mani1215919"

५.२.५.१.४. फ्रेजको कुनै पूरा शब्दलाई अङ्कले सङ्केत गरी तयार गरिएको पासवर्ड:

Give me liberty or give me death. Password: "GML^1518gmd"

५.२.५.१.५. केहि विराम चिन्हहरु तथा केहि विशेष चिन्हरु पयोग गरिएको पासवर्ड:

My aunt's name is Gita. Password: "m@n!79201"

The name of my favorite grandchild is Ravi. Password: "TNOMFG!181229"

५.२.५.२. माथि उल्लेख गरिएका केहि उदाहरणहरुमा झैं विराम चिन्हहरु प्रयोग गर्न कहिलेकाहिँ सजिलो पनि हुन सक्छ, जस्तो: प्रश्नवाचक फ्रेज प्रयोग गरिएको अवस्थाम (?) चिन्ह प्रयोग गर्न सकिन्छ । यदि फ्रेजमा संख्या पनि उल्लेख गरिएको भए $, %, र # जस्ता चिन्हहरु पासवर्डमा सजिलैसँग प्रयोग गर्न र संझिरहन पनि सजिलो हुन्छ । यदि फ्रेजमा "and", "to" वा "or" जस्ता

शब्दहरु प्रयोग भएका छन् भने तिनीहरुको सट्टा क्रमशः &, - ,वा / प्रयोग गर्न सकिन्छ । त्यस्तै पासवर्डहरुलाई / वा \ ले टुक्रयाउन पनि सकिन्छ । पासवर्डहरुमा बीचबीचमा वर्णमालाका साना तथा ठूला अक्षरहरु मिसाएर आफूलाई सम्झन सजिलो हुने गरी प्रयोग गर्न पनि भुल्नु हुदैन ।

६. पासवर्ड सुरक्षाका मानदण्डहरु

६.१. कार्यालयमा प्रयोग गरिने पासवर्डहरु व्यक्तिगत ISP एकाउन्ट, वैकल्पिक व्यवसाय वा लाभजन्य कारोवारका अन्य क्षेत्र गैरकार्यालयहरुमा प्रयोग गरिने एकाउन्टहरुमा प्रयोग गर्नु हुदैन । सम्भव भएसम्म विभिन्न कार्यालयको नामको पहुँचमा प्रयोग गरिएका भिन्न भिन्न एकाउन्टहरुमा एउटै पासवर्ड प्रयोग गर्नु हुदैन । उदाहरणको लागि इन्जिनियरिङ सिस्टममा एउटा पासवर्ड प्रयोग गरिएको भए आईटी सिस्टममा अलग्गै पासवर्ड प्रयोग गर्नु पर्दछ । त्यस्तै विन्डोज एनटी एकाउन्टमा प्रयोग गरिएको पासवर्ड युनिक्स एकाउन्टमा प्रयोग गर्नु हुदैन ।

६.२. संस्थागत पासवर्ड कसैलाई पनि दिनु हुदैन । आफ्नो निकटतम प्रशासन सहयोगी अथवा निजी सचिव समेतलाई आफ्नो पासवर्ड दिनु हुदैन । कुनै पनि प्रकारको पासवर्डहरुलाई संगठनको संवेदनशील र गोप्य सूचनाको रुपमा लिनु पर्दछ ।

६.३. यहाँ केहि गर्नै नहुने विषयहरुको सूची तयार गरिएको छ । पासवर्डको प्रयोग गर्दा यी विषयहरुलाई ध्यान दिएर तयार गर्नु पर्दछ ।

६.३.१. फोनबाट कुनै पनि अवस्थामा कसैलाई पनि पासवर्ड दिनु हुदैन ।

६.३.२. ईमेल सन्देशबाट कहिल्यैपनि पासवर्ड दिनु हुदैन ।

६.३.३. आफ्नो कार्यालय प्रमुख, परिवारका सदस्यहरु वा व्यवसायिक सहकर्मीहरुलाई समेत पासवर्ड दिनु हुदैन ।

६.३.४. कसैको अगाडि पासवर्डको विषयमा कुरा गर्नु हुदैन ।

६.३.५. पासवर्डको संकेतसम्म समेत खुल्ने गरी कसैसँग कुरा गर्नु हुदैन ।

६.३.६. कुनै पनि प्रकारको प्रश्नावली अथवा सुरक्षा फाराममा पासवर्ड खुलाउनु हुदैन ।

६.३.७. पासवर्डको कुनैपनि भागमा सामान्य चलनचल्तीका शब्द वा तिनको उल्टोबाट हिज्जे गरी बनाईएको शब्द प्रयोग गर्नु हुदैन ।

६.३.८. पासवर्डको कुनै अंशको रुपमा कुनै व्यक्ति अथवा स्थानको नाम प्रयोग गर्नु हुदैन ।

६.३.९. लग ईन नामको कुनै पनि भाग पासवर्डमा प्रयोग गर्नु हुदैन ।

६.३.१०. सजिलै थाहा पाउन सकिने खालका संख्याहरु जस्तोः टेलिफोन नम्वर, सामाजिक सुरक्षा परिचय नम्वर, जन्ममिति, वार्ड नम्वर आदि पासवर्डमा प्रयोग नगर्नु नै उपयुक्त हुन्छ ।

६.४. यहाँ केहि "कदापि" गर्न नहुने विषयहरुको सूची तयार गरिएको छ । पासवर्ड तयार गर्दा यी विषयहरुलाई विशेष ध्यान दिनु जरुरी छ ।

६.४.१. यूजर एकाउन्ट र पासवर्ड कहिल्यै पनि बाँड्नु हुदैन ।

६.४.२. एकभन्दा बढी एकाउन्टमा एउटै पासवर्ड कहिल्यै पनि प्रयोग गर्नु हुदैन ।

६.४.३. पासवर्ड कहिँ कतै लेख्नु हुँदैन । लेख्नै पर्ने अवस्था भएमा त्यसलाई आफ्नो मात्र पहुँच पुग्ने अत्यन्त गोप्य स्थानमा राख्नु पर्दछ ।

६.४.४. ईन्क्रिप्ट नगरी भण्डार गरिएको कुनै पनि तथ्याङ्कहरुमा पासवर्ड समावेश गर्नै हुदैन ।

६.४.५. इन्टरनेट ब्राउजरहरु (जस्तोः Internet Explorer, Mozilla Firefox, Google chrome, Safari आदि)मा ईमेल प्रोग्राम अथवा यस्तै प्रकारका अन्य कुनै एप्लिकेशन प्रोग्रामहरुमा प्राप्त हुने Remember password सुविधा प्रयोग गर्नु हुदैन ।

६.४.६. https:// को सट्टा http:// बाट वेव ब्राउजर ठेगाना शुरु भएका असुरक्षित लगईन हुने इन्टरनेट एकाउन्टहरुमा आफ्नो संगठन अथवा नेटवर्कको पासवर्ड प्रयोग गर्न हुदैन ।

६.५. कसैले पासवर्ड मागेको अवस्थामा उसलाई यी अभ्यासहरु हेर्न अथवा सूचना सुरक्षण विभाग/शाखाको कुनै व्यक्तिलाई सम्पर्क गर्न सुझाव दिनु उपयुक्त हुन्छ ।

६.६. इन्क्रिप्सन नगरीकन पासवर्डलाइ कम्प्यूटर वा कम्प्यूटरको कुनै पनि सिस्टममा राख्नु हुदैन । त्यस्तै कार्यालयको कुनै पनि ठाउँमा पासवर्ड लेखेर राख्ने काम गर्नु हुदैन । पासवर्डको सबैभन्दा सुरक्षित स्थान आफ्नो मष्तिष्क नै हो ।

६.७. प्रत्येक तीन महिनामा पासवर्ड परिवर्तन गर्न भुल्नु हुँदैन । सिस्टम लेभलका पासवर्डहरु भने हरेक महिनामा परिवर्तन गर्नु पर्दछ । सकेसम्म सबै प्रकारका पासवर्डहरुलाई पनि हरेक महिनामा परिवर्तन गर्नु राम्रो मानिन्छ ।

६.८. कुनै पासवर्ड कसैले गाहा पाएको आशंका भएमा सो को वारेमा सूचना सुरक्षण शाखा/विभागमा जानकारी गराईहाल्नु पर्दछ र तत्काल सम्पूर्ण पासवर्डहरु परिवर्तन गर्नु पर्दछ ।

६.९. सूचना सुरक्षण शाखा/विभागबाट कुनै संस्थाको आवधिक वा छड्के रुपमा पासवर्ड अनुमान वा क्रयाक गरी पासवर्डको वलियोपना जाँच्न सकिनेछ । यसरी परीक्षण गर्दा पासवर्ड

अनुमान सही भयो अथवा पासवर्ड क्र्याक भयो भने प्रयोगकर्ताले पासवर्ड परिवर्तन गरिहाल्नु पर्दछ ।

७. एप्लिकेशन निर्माणका मानदण्डहरु

७.१. एप्लिकेशन निर्माताहरुले आफ्ना प्रोग्राममा देहाय अनुसारको सुरक्षाको पूर्व सतर्कताहरुको बारेमा सावधानी अपनाउनु पर्दछ ।

७.१.१. समूह प्रयोगकर्ताको सट्टा व्यक्तिगत प्रयोगकर्ताको आधिकारिकताको लागि मद्दत पुऱ्याउने हुनु पर्दछ ।

७.१.२. क्लियर टेक्सट् अथवा त्यस्तै प्रकारको कुनैपनि सजिलै बदल्न वा मेट्न सकिने गरी पासवर्ड राख्नु हुदैन ।

७.१.३. धेरै व्यक्तिद्वारा प्रयोग गर्न सकिने खालको प्रोग्रामहरुको हकमा विशेष प्रकारको व्यवस्था प्रोग्रामहरुमा उपलब्ध गराउनु पर्दछ कि कुनै एक व्यक्तिले अर्को व्यक्तिले सम्पादन गरेका उक्त प्रकारका प्रोग्रामहरुको काममा उसको पासवर्ड थाहा नपाईकन नै पहुँच प्राप्त गर्न सकोस् ।

७.१.४. सम्भव भएसम्म प्रोग्राम तथा एप्लिकेशनहरु TACACS+, RADIUS, X-509 जस्ता LDAP सुरक्षा पुनर्स्थापनाहरुलाई सपोर्ट गर्ने हुनु पर्दछ ।

८. दूर पहुँच यूजरहरुका लागि पासवर्ड अथवा पासफ्रेजहरुको प्रयोग

८.१. कुनै पनि कार्यालयको नेटवर्कमा दूर पहुँच स्थापना गर्न या त एक पटकको पासवर्ड आधिकारिकता (Onetime Password Authentication) या बलियो पासफ्रेज प्रयोग गरिएको सार्वजनिक/निजी साँचो प्रणालीद्वारा नियन्त्रण हुनुपर्दछ ।

९. पासफ्रेजहरु

९.१. पासफ्रेजहरु सामान्यतः पब्लिक/प्राईभेट साँचो अथेन्टिकेशनका लागि प्रयोग गर्ने गरिन्छ । पब्लिक/प्राईभेट साँचो प्रणाली भनेको सबैले थाहा पाउने सार्वजनिक (पब्लिक) साँचो र प्रयोगकर्ताले मात्र थाहा पाउने निजी (प्राईभेट) साँचो बीचको गणितीय सम्वन्ध हो । पासफ्रेज विना प्राईभेट साँचो खोल्न युजरको पहुँच पुग्न सक्दैन ।

९.२. पासफ्रेजहरु पासवर्डहरु जस्तै हुदैनन् । पासफ्रेज भनेको पासवर्डको लामो भर्सन हो त्यसैले यो पासवर्डभन्दा बढी सुरक्षित हुन्छ । पासफ्रेज एकभन्दा बढी शब्दहरुका क्यारेक्टरहरुको उपयुक्त संयोजनबाट निर्माण गरिएको हुन्छ । यसै कारणले पासफ्रेज “शब्दकोष आक्रमण” बाट धेरै सुरक्षित रहन्छ ।

९.३. एउटा राम्रो पासवर्ड तुलनात्मक रुपमा लामो एवं वर्णमालाका ठूला तथा साना अक्षरहरु, अङ्कहरु तथा विराम चिन्हहरु संयुक्त रुपमा मिसाएर बनाईएको हुन्छ । एउटा राम्रो पासफ्रेजको उदाहरणः "The*?#>*0nThe!101was*&#!#Thismorning".

९.४. माथि उल्लेख भएका सम्पूर्ण नियमहरु पासफ्रेजको हकमा पनि अक्षरशः लागु हुन सक्दछन् ।

१०. एकपटकको पासवर्ड

१०.१. हाल एकपटक मात्र प्रयोग गरिने पासवर्डको प्रयोग हुने गरेको छ । त्यस्तो पासवर्डहरु यूएसवी टोकन तथा स्मार्ट कार्डहरुमा पाईन्छ । जसलाई ओटिपी स्मार्ट टोकन तथा सुरक्षित आइडि टोकन भनिन्छ । त्यस्तो पासवर्ड एकपटकमा एकपटक मात्र प्रयोग हुन्छ । अर्कोपटकको लागि स्वतः तयार भएको अर्को पासवर्ड प्रयोग गर्नु पर्ने हुन्छ । यसलाई कसैले पनि चोर्न नसक्ने भएकोले यस्तो प्रकारको पासवर्ड अत्यन्त सुरक्षित मानिन्छ ।

११. दण्ड सजायको व्यवस्था

११.१. अभ्यासहरुमा उल्लेखित विषयहरुको पालना नगर्ने कर्मचारीहरुलाई अनुशासनको कारवाहीको दायराबाट दण्ड वा सजाय गर्न सकिन्छ । सो कुरा कार्यालय वा संगठनको सूचना प्रविधि सम्वन्धी आचारसंहिता वा नीतिले निर्धारण गर्दछ ।

Secure Password Practices

(English Translation)

1. Introduction

1.1 A secure password practices is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A secure password practices is often part of an organization's official regulations and may be taught as part of security awareness training. The secure password practices may either be advisory or mandated by technical means.

2. Overview

2.1 Passwords are an important aspect of computer and information security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of organization's entire corporate network. As such, all organization's employees (including contractors, vendors and other external entities with access to organization systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.2 All employees that have access to organizational information systems must adhere to the password practices defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

3. Purpose

3.1 The purpose of these practices is designed, to protect organizational resources on the network by requiring strong password, to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. These practices may not hundred percent guarantees to secure the information system of the organization; however this practices will help to ensure only till the digital signature has not been introduced.

4. Scope

4.1 The scope of this practices includes all personnel who have or are responsible for an account (or any form of access that supports or

requires a password) on any system that resides at any organization facility, has access to the organization's network, information system and or stores any non-public organization information. But practices are not limited to a domain account and e-mail account.

5. Password Practices

5.1 General password Practices

5.1.1 All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

5.1.2 All production system-level passwords must be part of the Information Security administered global password management database.

5.1.3 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every two months. The recommended change interval is every month.

5.1.4 User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

5.1.5 Account lockout threshold - 4 failed login attempts.

5.1.6 Where SNMP (Simple Network Management Protocol) is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

5.1.7 All user-level and system-level passwords must conform to the guidelines described below.

5.1.8 Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.

5.1.9 Reset account lockout after - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value as of the date of writing this article is 20 minutes. This means if there are three bad attempts in 20 minutes, the account would be locked.

5.1.10 Account lockout duration - Some experts recommend that the administrator reset the account lockout so they are aware of possible break in attempts on the network. However this will cause a great deal

of additional help desk calls. Therefore depending on the situation, the account lockout should be between 30 minutes and 2 hours.

5.1.11 Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer".

5.1.12 Rules that apply to passwords apply to passphrases which are used for public/private key authentication.

5.1.13 Do not use the "Remember Password" feature of applications (e.g., Eudora, Out-Look, Netscape Messenger, Internet explorer and other browsers).

5.1.14 Do not access your organization information system, where your password is required, from the public network especially from the cyber café.

5.2 A. General Password Construction Guidelines

5.2.1 Passwords are used for various purposes at <Company Name>. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. Passwords having the following characteristics are generally considered as weak password:

5.2.1.1 The password contains less than fifteen characters

5.2.1.2 The password is a word found in a dictionary (English or foreign)

5.2.1.3 The password is a common usage word such as:

5.2.1.3.1 Names of family, pets, friends, co-workers, fantasy characters, etc.

5.2.1.3.2 Computer terms and names, commands, sites, companies, hardware, software.

5.2.1.3.3 The words "<Company Name>", "sanjose", "sanfran" or any derivation.

5.2.1.3.4 Birthdays and other personal information such as addresses and phone numbers.

5.2.1.3.5 Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

5.2.1.3.6 Any of the above spelled backwards.

5.2.1.3.7 Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

5.2.2 Strong passwords have the following characteristics:

5.2.2.1 Contain both upper and lower case characters (e.g., a-z, A-Z)

5.2.2.2 Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~- =\`{}[]:";'<>?,./)

5.2.2.3 Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).

5.2.2.4 Are not words in any language, slang, dialect, jargon, etc.

5.2.2.5 Are not based on personal information, names of family, etc.

5.2.2.6 Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

5.2.2.7 Passwords are case sensitive and the user name or login ID is not case sensitive.

5.2.3 Do not use either of these examples as passwords!

5.2.4 Creation of Password using phrase

5.2.4.1 Embed a word or part of a word within another.

5.2.4.2 Misspell a word deliberately especially if you use a word for part of your password.

5.2.4.3 Interleave two or more words.

5.2.4.4 Use a phrase that is personal to you and use the first, second, or third character in each word in each phrase. The Phrase can be a question and answer phrase. There can be several variants to this approach:

5.2.4.4.1 Use a phrase that has a number at the end of it.

5.2.4.4.2 After building the password, intermix the numbers and characters in a way that you can remember.

5.2.4.4.3 Put the answer part of the phase before the question.

5.2.4.4.4 Sometimes use capital letters, and sometimes use lower case letters. Use unusual capitalization in your phrase.

5.2.4.4.5 Use a numerical representation of the letters of the alphabet for part of your phrase or one word in your phrase. For example A is 1, B is 2, C is 3, etc.

5.2.4.4.6 Use punctuation or special characters in part of your phrase.

5.2.5 Some Examples

5.2.5.1 In these examples, threw in punctuation, usually at the end, but it could be applied at the beginning or in the case of passwords built with question/answer phrases, punctuation would work well in the middle.

5.2.5.1.1 Using a phrase with a number at the end of it. Example: My Favorite number is 333. Password: "MFNI333." or "yaus333." depending on whether the first or second character is used.

5.2.5.1.2 Using a phrase with a question and answer and numerical representation of the first letters of the answer. Example: My favorite song is "Dust in the Wind". Password: "MFSI492023!"

5.2.5.1.3 Using a phrase with a question and answer and numerical representation of all the letters in the answer. Examples:

The name of my favorite grandchild is Tim. Password: "tnomfgi#20913".

The name of my favorite aunt is Lois. Password: "Tnomfai1215919".

My aunt's name is Lois. Password: "%mani1215919".

5.2.5.1.4 Using a phrase with a numerical representation of one word in the phrase. Example: Give me liberty or give me death. Password: "GML^1516gmd".

5.2.5.1.5 Using a phrase with some punctuation or special characters. Example:

My aunt's name is Sita. Password: "m@n!S199201".

My first college friend is Ram. Password: "mfcfir!18113".

5.2.5.2 In many of the above examples, it is easy to throw in punctuation such as a ? when part of your phrase may be a question. If your phrase involves numbers or you work with numbers regularly, $, %, and # may be easy to use in your password and still remember. If your phrase uses the word "and" or "or", you can substitute "&" or "|". Also you can split your password with "/" or "\".Also remember to use upper and lower case letters in different parts of your password in ways that are easy for you to recall.

6. Password Protection Standards

6.1 Do not use the same password for <Company Name> accounts as for other non-<Company Name> access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various <Company Name> access needs. For example, select one

password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

6.2 Do not share organization's passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential organization information.

6.3 Here is a list of "don'ts" and "never":

6.3.1 Don't reveal a password over the phone to ANYONE

6.3.2 Don't reveal a password in an email message

6.3.3 Don't reveal or share a password even to the boss or family members or co-workers.

6.3.4 Don't talk about a password in front of others

6.3.5 Don't hint at the format of a password (e.g., "my family name")

6.3.6 Don't reveal a password on questionnaires or security forms

6.3.7 Don't use common words or reverse spelling of words in part of your password.

6.3.8 Don't use names of people or places as part of your password.

6.3.9 Don't use part of your login name in your password.

6.3.10 Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.

6.4 Here is a list of "never":

6.4.1 Never share a user account and password

6.4.2 Never use the same password for more than one account

6.4.3 Never write down a password, however if you have written to remember then keep it in secure place where only your access will be granted.

6.4.4 Never include a password in a non-encrypted stored document.

6.4.5 Never use the "Remember Password" feature of application programs such as internet browser (Internet Explorer, Mozilla Firefox, Google Chrome, and Safari etc), your e-mail program, or any program.

6.4.6 Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://

6.5 If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

6.6 Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

6.7 Change passwords at least once every three months (except system-level passwords which must be changed monthly). The recommended change interval is every month.

6.8 If an account or password is suspected to have been compromised, report the incident to Information Security and change all passwords.

6.9 Password cracking or guessing may be performed on a periodic or random basis by Information Security or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

7. Application Development Standards

7.1 Application developers must ensure their programs contain the following security precautions. The application:

7.1.1 Should support authentication of individual users, not groups.

7.1.2 Should not store passwords in clear text or in any easily reversible form.

7.1.3 Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

7.1.4 Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

8. Use of Passwords and Passphrases for Remote Access Users

8.1 Access to the organization Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

9. Passphrases

9.1 Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

9.2 Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is

typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

9.3 A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

9.4 All of the rules above that apply to passwords apply to passphrases.

10. One time password

10.1 Presently, people are using one time password to secure their system and transaction. These passwords are available in USB tokens or in smart cards that are called OTP Smart Card Tokens or secure ID tokens. The password produced by tokens can be used only in one time, next time new password will be produced. The OTP password is more secured than the password generated and maintained by other techniques.

11. Enforcement

10.1 Any employee found to have violated this practices may be subject to disciplinary action.