सूचना प्रविधि सुरक्षणको निम्ति अपनाउनु पर्ने विधिहरु

सूचना प्रविधिको प्रचुर प्रयोग मार्फत विभिन्न सरकारी, अर्ध सरकारी एवं गैर-सरकारी निकायहरुबाट सेवाग्राहीहरुलाई सहज-सुलभ ढङ्गबाट सेवा प्रवाह भइरहेको तथ्य विदितै छ। सूचना प्रविधिबाट सेवा प्रदान गर्दा समय र लागत दुबैमा वचत हुने तथा सेवाग्राहीले कार्यालयमा उपस्थिति हुनु नपरी घरबाटै सरकारी निकायका वेवसाइट, मोबाइल-एप, वेव-सर्भिस आदिको माध्यमबाट सेवा लिनसक्ने अवस्था छ। विशेष गरी, हाल सर्वव्यापी कोभिड-१९ महामारीले सूचना प्रविधिको महत्व र उपयोगितालाई अझै उजागर गरेको छ र दिनानुदिन निजी तथा सरकारी निकायहरुले यसलाई ग्रहण गर्ने क्रम बढ्दो रहेको छ। तर, सूचना प्रविधिको प्रयोगबाट सेवा प्रवाहमा जोखिम र चुनौतीहरु पनि रहेका कारण सुरक्षित सूचना प्रविधि प्रणाली प्रयोगमा ल्याउनु नितान्त आवश्यक रहेको छ। Hacking, Spam mail and Phishing, Ransom-ware, Distributed-Denial-of-Service जस्ता विभिन्न साइबर जोखिमहरु बढ्दो क्रममा रहेका छन्। विगतका केही दिनमा विभिन्न समुहबाट सरकारी निकायका वेवसाइट र वेव-एप्लिकेशनहरुमा आक्रमण भएको छ। त्यस्तै, निजि क्षेत्रतर्फ भायनेट र फुडमाण्डु प्रालि को तथ्यांक चोरी जस्ता घटनाहरु सामुन्ने आएका छन्। यस्ता बढ्दा साइबर आक्रमणका घटना प्रति यस मन्त्रालयको विशेष ध्यानाकर्षण भएको छ र मन्त्रालय अन्तर्गत रहेको **राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समुह** (National IT Emergency Response Team) ले विभिन्न सरोकारवाला निकायहरुको सहकार्यमा यसको सुक्ष्म अध्ययन गरिरहेको छ।

सूचना प्रविधि प्रयोगको विकल्प छैन। नेपाल सरकारको डिजिटल नेपाल निर्माण गर्ने महत्वकांक्षी योजनालाई सफल पार्दै आगामि दिनहरुमा सूचना प्रविधिको प्रयोगलाई तिव्रताका साथ विकास गर्दै लगिने कुरा नेपाल सरकारको नीति तथा कार्यक्रम र बजेट वक्तव्य समेतमा समावेश भइसकेको छ। यस परिप्रेक्षमा शैक्षिक क्षेत्र, बैङ्क तथा वित्तिय क्षेत्र, स्वास्थ्य क्षेत्र, दूरसञ्चार सेवा प्रदायकहरु लगायतका सबै सरकारी, अर्ध सरकारी र गैर सरकारी निकायहरुलाई निम्नानुसारका बुँदाहरुको अनुसरण गरी आ-आफ्नो सूचना प्रविधि संयन्त्रलाई थप सुदृढ गर्न यस सञ्चार तथा सूचना प्रविधि मन्त्रालय अनुरोध गर्दछ।

१) सबै सूचना प्रविधि प्रणालीहरुमा Secure Authentication को व्यवस्था गर्ने। यसकालागि 2-Factor Authentication र Non-Trivial Password Policy जस्ता कुराहरुमा ध्यान पुर्याउने।

२) ई-मेल मार्फत आउने Spam र Phishing Email सम्बन्धी आ-आफ्ना कर्मचारी लगायत सम्बन्धित सरोकारवालाहरुलाई सजग बनाउने। साथै, आफ्ना सेवाग्राहीहरु माझ पनि यस्ता प्रकृतिका ई-मेल आएमा चाल्नुपर्ने कदमका बारे जागरुकता फैलाउने। अनावश्यक, असम्बन्धित र अपरिचित व्यक्ति वा संस्थाहरुबाट आएका इ-मेल त्यसको आधिकारिकता पुष्टि नभएसम्म खोल्दै नखोल्ने अभ्यासको विकास गर्ने।

३) आफ्ना सूचना प्रविधि संयन्त्र i.e. Database, Application Libraries, Operating System, Kernel etc. लाई नियमित रुपमा अपडेट गर्ने। साथै, Anti-virus जस्ता प्रणालीहरु समेत नियमित अपडेट गरी प्रयोग गर्ने।

४) Operating System सकेसम्म Latest Version को Genuine मात्र प्रयोग गर्ने र समय समयमा Patch हरु Update गरिरहने। Operating System को सबैभन्दा उच्च अधिकार प्राप्त अकाउन्ट अर्थात root वा administrator एकाउन्टमा सकेसम्म log-in disable गर्ने र यस्तो User सम्बन्धित निकायको एकजना सूचना प्रविधि सम्बन्धी हेर्ने Supervisor ले मात्र प्रयोग गर्ने गरी व्यवस्था मिलाउने।

५) आफ्नो निकायमा प्रयोग भएका सबै Desktop, Laptop लगायतका उपकरणहरुको USB, CD/DVD लगायतका Port हरु बन्द गरी External Device मा/बाट कपि गर्न नसकिने गरी व्यवस्था गर्ने र यदि संस्थाभित्र File, Document वा कुनै Information share गर्नु पर्ने अवस्था हुने भएमा, त्यसको लागि Active Directory को प्रयोग गर्ने।

६) आफ्नो Firewall Policies हरु खुकुलो रहेको नरहेको विषयमा अध्ययन गरी आवश्यक परिमार्जन गर्ने। जस्तै, अनावश्य Port हरु बन्द गर्ने, SSH/Telnet/RDP जस्ता Remote-access ports हरुमा Brute-force आक्रमण जोगाउन max-failed-tries-within-time-limit परिभाषित गर्ने, आवश्यकता अनुसार IP Blacklisting / IP Whitelisting गर्ने, Port-Knocking को व्यवस्था गर्ने।

७) डाटावेसमा रहेका अतिगोप्य डाटा (जस्तै प्रयोगकर्ताको पासवर्ड) लाई Hash वा Encrypt गरेर राख्ने। सम्भव भएसम्म डाटालाई समेत Hash वा Encrypt गरेर भण्डारण गर्ने गरी व्यवस्था मिलाउने।

८) सबै URL मा अनिवार्य रुपमा Secure Socket Layer(SSL) को प्रयोग गर्ने।

सूचना प्रविधि सुरक्षणको निम्ति अपनाउनु पर्ने विधिहरु

९) आफ्नो सूचना प्रविधि प्रणालीहरुलाई विशेषज्ञ मार्फत सुरक्षा परिक्षण गराउने र परिक्षणको प्रतिवेदन अनुसारका सबै आक्रमण विन्दुहरुलाई तत्काल समाधान गर्ने। सुरक्षण परिक्षणको निम्ति सूचना प्रविधि विभागको समेत सहयोग लिन सकिने र आवश्यकतानुसार तेस्रो पक्षबाट समेत सुरक्षण परिक्षण गराउने।

१०) आफ्ना सबै तथ्याङ्कहरु नियमित रुपमा Backup and Archiving गर्ने। अनिवार्य रुपमा सकेसम्म दैनिक रुपमा कम्तिमा एक प्रति डाटा तथा Application को CD/DVD, External Hard Drive वा यस्तै कुनै External Media मा Backup समेत गरी छुट्टै ठाउँमा offline सुरक्षित भण्डारण गरी राख्ने।

११) अत्यावश्यक तथा संवेदनशील सूचना प्रविधि प्रणाली सञ्चालन गरिरहेका निकायहरुले, सञ्चालनमा आइरहेको प्रणाली कुनै कारणले सञ्चालन हुन नसक्ने अवस्था आएमा तुरुन्त सञ्चालनमा ल्याउने सक्ने गरी कम्तिमा एउटा Backup प्रणालीको व्यवस्था गर्ने।

१२) कुनै पनि कारणले आफ्नो निकायमा सञ्चालित सूचना प्रविधि प्रणालीमा कुनै पनि किसिमको खरावी आए पनि सेवा प्रवाहमा कुनै अवरोध नहुने गरी तयारी अवस्थामा हुने व्यवस्था मिलाउने।

१३) सूचना प्रविधि निर्माण तथा प्रयोग गर्दा यस अघि सञ्चार तथा सूचना प्रविधि मन्त्रालय, सूचना प्रविधि विभाग, राष्ट्रिय सूचना प्रविधि केन्द्र, नेपाल दूरसञ्चाल प्राधिकरण, नेपाल राष्ट्र वैक लगायतका निकायहरुबाट सूचना प्रविधिसँग सम्बन्धित विभिन्न विषयमा निर्मित मापदण्ड तथा परिपत्रहरुको अनिवार्य रुपमा पालना गर्ने।

अन्ततः आफ्नो सूचना प्रविधि संयन्त्रहरुमा अनाधिकृत पहुँच भई तथ्याङ्कहरु चोरी भएको, Ransomeware वा Malware आक्रमण भएको, DDoS आक्रमण भएको वा अन्य कुनैपनि सङ्कास्पद गतिविधि भएको सम्बन्धी **जानकारी राष्ट्रिय सूचना प्रविधि आकस्मिक सहायता समुहलाई** nitert@mocit.gov.np मा जानकारी दिन सक्नुहुनेछ।