গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

ডিজিটাল ডিভাইস, ইন্টারনেট এবং তথ্য রক্ষণাবেক্ষণ ও নিরাপত্তা নির্দেশিকা, ২০২০

মন্ত্রিপরিষদ বিভাগ

মাঘ ১৪২৬/জানুয়ারি ২০২০

ডিজিটাল ডিভাইস, ইন্টারনেট এবং তথ্য রক্ষণাবেক্ষণ ও নিরাপত্তা নির্দেশিকা, ২০২০

১. প্রেক্ষাপট :

তথ্য-প্রযুক্তি নির্ভর বিশ্বায়নের যুগে মানুষের দোরগোড়ায় সেবা পৌঁছে দিতে প্রধানতম একটি মাধ্যম হলো ইন্টারনেট। দৈনন্দিন জীবনে তথ্যপ্রযুক্তি ও ইন্টারনেটের নির্ভরশীলতা বাড়ার সঙ্গে সঙ্গে কম্পিউটার ও ইন্টারনেটে রক্ষিত দাপ্তরিক ও গুরুত্বপূর্ণ তথ্যসমূহের নিরাপত্তার ঝুঁকিও বৃদ্ধি পেয়েছে। সচিবালয় নির্দেশমালা, ২০১৪-এ সাইবার নিরাপত্তা ও তথ্য নিরাপত্তার ওপর গুরুত্বারোপ করা হয়েছে। ডিজিটাল বাংলাদেশ অর্থাৎ রূপকল্প ২০২১ বাস্তবায়নে তথ্য-উপাত্ত ডিজিটাইজেশনের সঙ্গে সঙ্গে এর নিরাপত্তা বিধানের প্রতি সর্বোচ্চ সতর্কতা অবলম্বন জরুরি হয়ে পড়েছে।

নিরাপদ ইন্টারনেট ব্রাউজিং-এর কলাকৌশল না জেনে ইন্টারনেট ব্যবহার করার ফলে সম্প্রতি সরকারি দপ্তরসমূহে ব্যবহৃত অনলাইন সিস্টেম, ডিজিটাল ডিভাইস ও ডিভাইসে সংরক্ষিত গুরুত্বপূর্ণ তথ্যসমূহ বিভিন্ন ধরণের সাইবার আক্রমণের শিকার হচ্ছে। এ লক্ষ্যে সকল সরকারি প্রতিষ্ঠানের ডিজিটাল ডিভাইস ও তথ্য সুষ্ঠুভাবে সংরক্ষণসহ নিরাপত্তা ব্যবস্থা গ্রহণের জন্য 'ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নির্দেশিকা, ২০২০' প্রণয়ন করা হলো। এ নির্দেশিকা অনুসরণের মাধ্যমে ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তার সঙ্গে সংশ্লিষ্ট কর্মকর্তা-কর্মচারীগণ নিরাপত্তায় অধিকতর দায়িত্বশীল ভূমিকা পালন করতে সক্ষম হবেন।

২. সংজ্ঞা:

বিষয় বা প্রসঙ্গের পরিপন্থী কোনো কিছু না থাকলে, এই নির্দেশিকায়-

(১) "ডিজিটাল তথ্য" অর্থ টেক্সট, ইমেজ, অডিও বা ভিডিও আকারে প্রস্তুত তথ্য, জ্ঞান, ঘটনা, ধারণা বা নির্দেশাবলী যা কম্পিউটার প্রিন্ট আউট, ম্যাগনেটিক বা অপটিক্যাল স্টোরেজ মিডিয়া, পাঞ্চকার্ড, পাঞ্চ টেপসহ যে কোন আকারে বা বিন্যাসে কম্পিউটার সিস্টেম অথবা কম্পিউটার নেটওয়ার্কে প্রক্রিয়াজাত করা হয়েছে, হচ্ছে বা হবে অথবা অভ্যন্তরীণভাবে যা কোন কম্পিউটার স্মৃতিতে সংরক্ষিত;

(২) "ডিজিটাল ডিভাইস" অর্থ কোনো ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক, অপটিক্যাল বা তথ্য প্রক্রিয়াকরণ যন্ত্র বা সিস্টেম যা ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক বা অপটিক্যাল ইমপাল্স ব্যবহার করে যৌক্তিক, গাণিতিক এবং স্মৃতি বিষয়ক কার্যক্রম সম্পন্ন করে অথবা কোন ডিজিটাল সিস্টেম বা নেটওয়ার্কের সঙ্গে সংযুক্ত হয়ে সকল ইনপুট, আউটপুট, প্রক্রিয়াকরণ, সঞ্চিত, যোগাযোগ ইত্যাদি কার্যক্রম সম্পন্ন করে তা এর অন্তর্ভুক্ত হবে;

(৩) "তথ্য" অর্থ এ নির্দেশিকার অনুচ্ছেদ-২ (১) এ বর্ণিত ডিজিটাল তথ্য;

(৪) "তথ্য নিরাপত্তা নিরীক্ষা" অর্থ তথ্য যথাযথভাবে সংরক্ষণ করা হয়েছে কি না তা পর্যবেক্ষণ এবং মূল্যায়ন;

(৫) "ভাইরাস" অর্থ এক ধরনের কম্পিউটার প্রোগ্রাম বা কোড বা নির্দেশনা যা কোন কম্পিউটার বা ডিজিটাল ডিভাইসে সংক্রমণের ফলে স্বয়ংক্রিয়ভাবে তথ্য পরিবর্তন, বিনাশ, ক্ষতি বা এর কার্যসম্পাদনের দক্ষতায় বিরূপ প্রভাব বিস্তার করে;

(৬) "ম্যালওয়ার" অর্থ এমন কোনো কম্পিউটার বা ডিজিটাল নির্দেশ, তথ্য-উপাত্ত, প্রোগ্রাম বা এ্যাপস যা -

(ক) কোনো কম্পিউটার বা ডিজিটাল ডিভাইস কর্তৃক সম্পাদিত কার্যকে পরিবর্তন, বিকৃত, বিনাশ, ক্ষতি বা ক্ষুন্ন করে বা এর কার্য সম্পাদনে বিরূপ প্রভাব বিস্তার করে;

(খ) নিজেকে অন্য কোনো কম্পিউটার বা ডিজিটাল ডিভাইসের সাথে সংযুক্ত করে উক্ত কম্পিউটার বা ডিজিটাল ডিভাইসের কোনো প্রোগ্রাম, তথ্য-উপাত্ত বা নির্দেশ কার্যকর করার বা কোনো কার্য সম্পাদনের সময় স্বপ্রণোদিতভাবে ক্রিয়াশীল হয়ে উঠে এবং উক্ত কম্পিউটার বা ডিজিটাল ডিভাইসে কোনো ক্ষতিকর পরিবর্তন বা ঘটনা ঘটায়; এবং

(গ) কোনো ডিজিটাল ডিভাইসের তথ্য চুরি বা তাতে স্বয়ংক্রিয় প্রবেশের সুযোগ সৃষ্টি করে।

(৭) "সাইবার ঘটনা" অর্থ সাইবার নিরাপত্তা সংক্রান্ত বৈরী পরিস্থিতিকে বুঝাবে যেখানে নিরাপত্তা ব্যবস্থা ও নীতিমালা ভঙ্গ করে অনুনমোদিত প্রবেশ সংঘঠিত হয়। কোনো সেবা প্রদান বন্ধ বা ব্যাহত হয় এবং কম্পিউটার ও কম্পিউটার সিস্টেম অনুনমোদিত ব্যবহারের মাধ্যমে তথ্য পরিবর্তন, তথ্য-উপাত্ত প্রক্রিয়াকরণ ও সংগৃহীত হয়;

(৮) "সামাজিক যোগাযোগ মাধ্যম" অর্থ কম্পিউটার বা ডিজিটাল ডিভাইসে ইন্টারনেট ব্যবহারের মাধ্যমে পারস্পরিক যোগাযোগের উদ্দেশ্যে তথ্য-উপাত্ত (টেক্সট, ইমেজ, অডিও, ভিডিও ইত্যাদি) আদান-প্রদানের একটি প্ল্যাটফরম; এবং

(৯) "সরকারি প্রতিষ্ঠান" অর্থ কোন আইন, বিধি বা সরকারি আদেশ বলে প্রতিষ্ঠিত প্রতিষ্ঠান, সংবিধিবদ্ধ সংস্থা, অথবা সরকারের মালিকানা বা নিয়ন্ত্রণাধীন কোনো প্রতিষ্ঠান বা কর্তৃপক্ষ।

৩. উদ্দেশ্য:

(১) ডিজিটাল তথ্য সম্পর্কে ধারণা, সংরক্ষণ এবং নিরাপত্তা বিষয়ে সক্ষমতা ও সচেতনতা বৃদ্ধি করা;

(২) ডিজিটাল ডিভাইস, সফটওয়্যার ও নেটওয়ার্ক যথাযথভাবে পরিচালন, সংরক্ষণ ও নিরাপদ রাখা; এবং

(৩) ইন্টারনেট, ওয়েবসাইট ও সামাজিক যোগাযোগ মাধ্যম ব্যবহারে সচেতনতা বৃদ্ধি করা।

৪. নির্দেশিকার পরিধি:

এ নির্দেশিকাটি সকল সরকারি প্রতিষ্ঠানে ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নিশ্চিতকরণের ক্ষেত্রে প্রযোজ্য হবে।

৫. ডিজিটাল ডিভাইস ও তথ্য ব্যবস্থাপনা:

৫.১. ইনভেন্টরি তৈরি:

সুষ্ঠু তথ্য ব্যবস্থাপনার জন্য প্রতিষ্ঠানের ডিজিটাল ডিভাইস এবং তথ্যের ইনভেন্টরি প্রস্তুত করা প্রয়োজন। ইনভেন্টরি প্রস্তুত করার সময় সকল সম্পদের গুরুত্ব বিবেচনায় এনে তালিকাভুক্ত করতে হবে। ইনভেন্টরিতে সম্পদের ধরন, আকার, অবস্থান, ব্যাকআপ, লাইসেন্স বিষয়ক তথ্য, প্রতিষ্ঠানের কাছে এর প্রয়োজনীয়তা এবং মূল্যসহ অন্যান্য প্রয়োজনীয় সকল তথ্য অন্তর্ভুক্ত রাখতে হবে।

৫.২. তথ্য শ্রেণিকরণ:

সরকারি বিধি-বিধানের আলোকে তথ্যের গোপনীয়তা, প্রয়োজনীয়তা, অগ্রাধিকার ইত্যাদি বিবেচনাপূর্বক তথ্য শ্রেণিকরণ নিশ্চিত করতে হবে।

Shurooz

৫.৩. তথ্য নিরাপত্তার কৌশলসমূহ:

(ক) তথ্য নিরাপত্তা কৌশল প্রণয়নের নিমিত্ত জনবল ও প্রযুক্তির সমন্বয়ে কর্ম-পরিকল্পনা গ্রহণ করতে হবে।

(খ) তথ্য নিরাপত্তা সম্পর্কিত নতুন নতুন হুমকি/ঝুঁকি নিরসনের লক্ষ্যে নিয়মিত প্রতিষ্ঠানের গৃহীত কৌশলসমূহ পরীক্ষা করে দেখতে হবে। তথ্য নিরাপত্তা কৌশলের পদ্ধতিসমূহ সম্পর্কে ধারণা নিয়ে প্রতিষ্ঠানের প্রয়োজন অনুযায়ী অনুশীলনযোগ্য টেকসই পদ্ধতির নিরাপত্তা কৌশল প্রণয়ন করতে হবে।

(গ) তথ্য নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে যন্ত্রপাতির নিয়ন্ত্রণ, প্রবেশাধিকার নিয়ন্ত্রণ, ভৌত ও পরিবেশগত নিরাপত্তা ব্যবস্থা, সফটওয়্যারের নিরাপত্তা ও ব্যাক-আপ ব্যবস্থা, নেটওয়ার্ক নিরাপত্তা-ব্যবস্থাপনা, ক্রিপ্টোগ্রাফিক নিয়ন্ত্রণ, প্রক্রিয়াকরণ ইত্যাদি বিষয়সমূহ গুরুত্বের সঙ্গে বিবেচনা করতে হবে।

(ঘ) হার্ডওয়্যার, সফটওয়্যার, নেটওয়ার্ক ইত্যাদি সেবা গ্রহণ কার্যক্রমে ব্যবহারের Service Level Agreement নিশ্চিত হতে হবে।

(ঙ) যথাসম্ভব ডিজিটাল সিগনেচার ব্যবহার নিশ্চিত করতে হবে।

৫.৪. ডিজিটাল ডিভাইস সুরক্ষায় করণীয়:

(ক) কম্পিউটারের সঙ্গে ইউপিএস ব্যবহার করা;

(খ) কম্পিউটার/ল্যাপটপ/ট্যাব/মোবাইল ইত্যাদি ডিজিটাল ডিভাইসসমূহ অবশ্যই পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

(গ) ডেস্ক থেকে উঠে যাবার সময় ব্যবহৃত কম্পিউটার/ল্যাপটপ সিস্টেম লক করে যাওয়া;

(ঘ) কম্পিউটার/ল্যাপটপ সংরক্ষিত গুরুত্বপূর্ণ ফাইলসমূহ zip করে ব্যকআপ রাখা;

(ঙ) কম্পিউটার/ল্যাপটপে ইউএসবি পোর্টের ব্যবহার নিয়ন্ত্রণ করা;

(চ) কম্পিউটার/ল্যাপটপ/মোবাইলে লাইসেন্স-ভার্সন এন্টিভাইরাস সফটওয়্যার ব্যবহার করা এবং নিয়মিত আপডেট রাখা;

(ছ) সংশ্লিষ্ট ডিজিটাল ডিভাইসে Biometric Authentication (Finger Print, Scans Option ইত্যাদি) থাকলে তা Enable রাখা;

(জ) কম্পিউটার/ল্যাপটপ/মোবাইলে অপ্রয়োজনীয় Service বন্ধ রাখা;

(ঝ) ডেস্কটপ/ল্যাপটপ/মোবাইল/ট্যাবে অননুমোদিত সফটওয়্যার ইনস্টল না করা;

(ঞ) ডেস্কটপ/ল্যাপট/মোবাইল/ট্যাব অপরিচিত কোন ব্যক্তিকে ব্যবহার করতে না দেয়া;

(ট) পেনড্রাইভ, এক্সটার্নাল হার্ডডিস্ক, মেমরি কার্ড, সিডি/ডিভিডি ডিস্ক ইত্যাদি ভাইরাস স্ক্যান করে ব্যবহার করা;

(ঠ) গুরুত্বপূর্ণ ডকুমেন্টসমূহ পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

(ড) লাইসেন্সকৃত আপডেটেড অপারেটিং সিস্টেম, এন্টিভাইরাস, এপ্লিকেশন সফট্ওয়্যার ইত্যাদি ব্যবহার করা;

(ড) অপারেটিং সিস্টেমে ফায়ারওয়াল চালু রাখা;

(ণ) প্রয়োজন না হলে ডিভাইসের সাথে সংযুক্ত যোগাযোগ মাধ্যম (ব্লু-টুথ, ওয়াই-ফাই, হটস্পট, ইনফ্রারেড ইত্যাদি) বন্ধ রাখা;

(ত) ব্যাকআপ ফাইলসমূহ অপারেটিং সিস্টেম ড্রাইভ (c:/, ডেস্কটপ, ডাউনলোড ইত্যাদি) ব্যতীত অন্য ড্রাইভে সংরক্ষণ করা;

(থ) তথ্য-উপাত্ত নিয়মিত বিকল্প স্টোরেজ ডিভাইস এ ব্যাক-আপ রাখা;

(দ) নিরাপত্তার বিষয়ে নিশ্চিত না হয়ে ফ্রি সফট্ওয়্যার ডাউনলোড করা থেকে বিরত থাকা;

Sherzor

(ধ) নিয়মিত ডিজিটাল ডিভাইস পরিষ্কার পরিচ্ছন্ন রাখা;

(ন) হার্ডওয়্যারের কোয়ালিটি টেস্ট নিশ্চিত করা;

(প) কম্পিউটার/ল্যাপটপ/ট্যাবের physical security নিশ্চিত করা;

(ফ) কম্পিউটার/ল্যাপটপ/ট্যাবের কাজ শেষ হওয়া মাত্র shut down কমান্ড দিয়ে বন্ধ করা।

(ব) Memory Card, Pen drive, HDD, CD নষ্ট হলে তা ফেলে না দিয়ে বা বিক্রি না করে প্রচলিত বিধি-বিধান অনুসরণ করে ধ্বংস করা যেতে পারে; এবং

(ভ) নিয়মিত file system error checking, disk cleanup, disk defragment করা।

৫.৫. সফটওয়্যারের নিরাপত্তায় করণীয়:

(ক) সফটওয়্যার প্রস্তুতের সময় সংশ্লিষ্ট বাংলাদেশ ন্যাশনাল ডিজিটাল আর্কিটেকচার ফ্রেমওয়ার্ক (BNDA) যথাযথভাবে অনুসরণ করা;

(খ) বাংলাদেশ কম্পিউটার কাউন্সিল কর্তৃক সফটওয়্যারের কোয়ালিটি টেস্ট নিশ্চিত করে ব্যবহার করা;

(গ) সফটওয়্যারে ইউজার পাসওয়ার্ড এনক্রিপ্ট করে রাখা;

(ঘ) ওয়েব এপ্লিকেশন নিরাপত্তার জন্য Secured Socket Layer (SSL) সার্টিফিকেশন ব্যবহার করা;

(ঙ) সফটওয়্যারের Vulnerability নিয়মিত পরীক্ষা করা এবং প্রাপ্ত ফলাফলের ভিত্তিতে প্রয়োজনীয় পদক্ষেপ নেয়া;

(চ) সফটওয়্যার বা ওয়েবসাইটে অ্যাডমিন ইউজারের পাসওয়ার্ড নিয়মিত পরিবর্তনের অপশন রাখা;

(ছ) সফটওয়্যার বা ওয়েবসাইটের লগইন পাতায় অধিক নিরাপত্তার জন্য 2-Factor Authentication ব্যবস্থা রাখা;

(জ) লগ-ইন এলার্ট ব্যবহার করা;

(ঝ) প্রস্তুতকৃত সফটওয়্যারের সোর্সকোড, ডাটাবেইজ এবং ডকুমেন্টেশন সংরক্ষণ নিশ্চিত করা; এবং

(ঞ) সফটওয়্যারের চুক্তির মেয়াদ শেষ হওয়ার পূর্বেই যথাসময়ে প্রয়োজনীয় ব্যবস্থা গ্রহণ করা।

৫.৬. সর্বক্ষেত্রে পাসওয়ার্ড ব্যবস্থাপনায় করণীয়:

(ক) ব্যবহৃত পাসওয়ার্ড কমপক্ষে ৮ ডিজিট হওয়া সমীচীন (পাসওয়ার্ড কমপক্ষে একটি বড় অক্ষর, একটি ছোট অক্ষর, সংখ্যা ও বিশেষ চিহ্নের সমন্বয়ে থাকা প্রয়োজন);

(খ) পাসওয়ার্ড তৈরি ও রিকভারি করার সময় সিকিউরিটি চেকের ব্যবস্থা রাখা;

(গ) অন্যকোনো ব্যক্তির সঙ্গে ব্যবহৃত পাসওয়ার্ডটি শেয়ার না করা এবং কেউ জানতে পারে এমন কোথাও লিখে না রাখা;

(ঘ) পাসওয়ার্ড তৈরিতে নিজের নাম, জন্ম তারিখ ও অন্যান্য ব্যক্তিগত তথ্য ব্যবহারে বিরত থাকা;

(ঙ) নিয়মিত (অন্তত ২/৩ মাস পর পর) পাসওয়ার্ড পরিবর্তন করা; এবং

(চ) পাসওয়ার্ড পরিবর্তনের সময় সিস্টেমে স্বয়ংক্রিয় সতর্ক বার্তা প্রদর্শন করার ব্যবস্থা রাখা।

৫.৭. লোকাল এরিয়া নেটওয়ার্ক (LAN) সুরক্ষায় করণীয়:

(ক) LAN-এ অননুমোদিত ব্যক্তির ডিজিটাল ডিভাইস ব্যবহার নিয়ন্ত্রণ করা;

(খ) নেটওয়ার্ক সুরক্ষার জন্য ম্যানেজেবল সুইচ, ফায়ারওয়্যাল, রাউটার ইত্যাদি ব্যবহার করা;

(গ) ডিজিটাল ডিভাইসে রিমোট অ্যাকসেসের বিষয়ে সতর্ক থাকা;

Sheree2

(ঘ) সার্ভার/কম্পিউটার/ল্যাপটপের কোন ড্রাইভ, ফোল্ডার, ফাইল ইত্যাদি অননুমোদিত কারও সঙ্গে শেয়ার না করা;

(ঙ) সিস্টেম বা নেটওয়ার্কে বিদ্যমান নিরাপত্তা ব্যবস্থার কার্যকারিতা যাচাইয়ের জন্য নিয়মিত পরীক্ষা করা;

(চ) নিয়মিত নেটওয়ার্ক মনিটরিং সিস্টেম পর্যবেক্ষণ ও বিশ্লেষণ করা; এবং

(ছ) সার্ভারসহ অন্যান্য গুরত্বপূর্ণ এ্যাপ্লিকেশনসমূহ ল্যান ব্যবস্থাপনা থেকে পৃথক নিরাপত্তা ব্যবস্থাপনায় রাখা।

৫.৮. ইন্টারনেট ব্যবস্থাপনায় করণীয়:

(ক) সরকার অনুমোদিত আইএসপি প্রতিষ্ঠান হতে ইন্টারনেটের সংযোগ নেওয়া;

(খ) যথাযথ ব্যবস্থাপনার মাধ্যমে ইন্টারনেট ব্যান্ডউইথের সর্বোচ্চ ব্যবহার নিশ্চিত করা;

(গ) ইন্টারনেট সংযোগের ক্ষেত্রে অনুমোদিত ডিভাইস ব্যবহার নিশ্চিত করা;

(ঘ) ব্রাউজারে পাসওয়ার্ড স্থায়ীভাবে সংরক্ষণ না করা;

(ঙ) নিয়মিত ব্রাউজার আপডেট রাখা;

(চ) ফ্রি প্রক্সি সাইট ব্যবহার থেকে বিরত থাকা;

(ছ) পাবলিক হটস্পট থেকে অনলাইন অ্যাকাউন্ট ব্যবহারের সময় সতর্কতা অবলম্বন করা;

(জ) ওয়াই-ফাই রাউটার পাসওয়ার্ড নিয়মিত পরিবর্তন করা;

(ঝ) প্রসিদ্ধ ওয়েবসাইট ছাড়া অন্য সোর্স থেকে ফ্রি সফটওয়্যার ডাউনলোড করা থেকে বিরত থাকা।

(ঞ) ব্রাউজার হিস্টোরি ও কম্পিউটার ক্যাশ মেমরি নিয়মিত পরিস্কার করা; এবং

(ট) দাপ্তরিক ইন্টারনেট ব্যবহারের ক্ষেত্রে আগত অতিথিদের Captive Portal এর মাধ্যমে ভেরিফাই করা।

৫.৯. ই-মেইল ব্যবস্থাপনায় করণীয়:

(ক) দাপ্তরিক কাজে সরকারি ই-মেইল ব্যবহার নিশ্চিত করা;

(খ) ই-মেইল সিকিউরিটি গেটওয়ে ব্যবহার নিশ্চিত করা;

(গ) ই-মেইল ব্যবহার শেষে লগ আউট হওয়া;

(ঘ) ভাইরাস বা ম্যালওয়্যার থেকে সুরক্ষায় ই-মেইলে আগত .exe, .bat, .vbs, .scr ইত্যাদি ফাইল খোলা থেকে বিরত থাকা;

(ঙ) সন্দেহজনক ই-মেইল বা সংযুক্তি না খোলা;

(চ) ই-মেইল থেকে নিয়মিত অপ্রয়োজনীয় তথ্যাদি অপসারণ করা এবং

(ছ) খুব বেশি জরুরি না হলে অন্যের কম্পিউটার থেকে ই-মেইল, সোস্যাল মিডিয়া প্ল্যাটফরম ইত্যাদিতে লগ-ইন করা থেকে বিরত থাকা;

(জ) ই-মেইলে আগত অবাঞ্ছিত মেইল "স্পট অফার", "লটারি মানি", "ফ্রি লোন", "এ্যাওয়ার্ড" ইত্যাদি নানা ধরনের আকর্ষণীয়, প্রণোদনামূলক মেইলে ক্লিক না করে তাৎক্ষণিকভাবে এ সকল ই-মেইল ডিলিট করে দেওয়া;

(ঝ) অন্যের কম্পিউটারে ই-মেইল, সোস্যাল মিডিয়া বা অন্য কোনো সাইটে লগ-ইন করার ক্ষেত্রে ব্রাউজারে "Incognito" মোড বা প্রাইভেট মোড ব্যবহার করা;

(ঞ) সরকারি ই-মেইল নীতিমালা ২০১৮ অনুসরণ করা;

(ট) ই-মেইলের গুরুত্বপূর্ণ কনটেন্টসমূহ পৃথক সার্ভারে আর্কাইভ করে রাখা; এবং

(ঠ) ই-মেইলের পাসওয়ার্ড ব্যবস্থাপনার ক্ষেত্রে এ নির্দেশিকার ৫.৬ এ বর্ণিত নির্দেশাবলি অনুসরণ করা।

৫.১০. সার্ভার কক্ষ সুরক্ষায় করণীয়:

(ক) সার্ভার কক্ষে প্রবেশে কঠোর নিয়ন্ত্রণ ব্যবস্থা বজায় রাখা;

(খ) প্রয়োজনে নিরাপত্তাকর্মীর মাধ্যমে সার্ভার কক্ষের সার্বক্ষণিক নিরাপত্তা নিশ্চিত করা;

(গ) সার্ভার কক্ষের দরজায় উন্নতমানের লকের ব্যবস্থা রাখা;

(ঘ) সার্বক্ষণিক সিসিটিভি'র মাধ্যমে নজরদারির ব্যবস্থা রাখা;

(ঙ) ভিজিটর অথবা ভেন্ডরদের সার্ভার কক্ষে প্রবেশের তথ্য রেজিস্টারে লিপিবদ্ধ রাখা;

(চ) ফিঙ্গার প্রিন্টসহ অন্যান্য বায়োমেট্রিক সিকিউরিটি সিস্টেমের ব্যবস্থা রাখা;

(ছ) সার্ভার কক্ষে নিরবচ্ছিন্ন বিদ্যুৎ সরবরাহ ও শীতাতপ নিয়ন্ত্রণের ব্যবস্থা রাখা;

(জ) স্বয়ংক্রিয় অগ্নিনির্বাপন সিস্টেমের ব্যবস্থা রাখা;

(ঝ) Environment Monitoring System ব্যবস্থা রাখা; এবং

(ঞ) বন্যা, অগ্নিকাণ্ড, ভূমিকম্প ইত্যাদি প্রাকৃতিক দুর্যোগ বিবেচনায় রেখে সার্ভার কক্ষের অবস্থান নির্ধারণ করা।

৫.১১.সার্ভার সুরক্ষায় করণীয়:

(ক) সার্ভারের সঙ্গে অনলাইন ইউপিএস-এর ব্যবহার নিশ্চিত করা;

(খ) সার্ভার অবশ্যই পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

(গ) সার্ভারে ইউএসবি পোর্টের ব্যবহার নিয়ন্ত্রণ করা;

(ঘ) সার্ভার-কে ভাইরাস, স্পাইওয়্যার, মালওয়্যার, অ্যাডওয়্যার এবং অন্যান্য আক্রমণ মুক্ত রাখার জন্য লাইসেন্স-ভার্সন এন্টিভাইরাস সফটওয়্যার ব্যবহার করা, এন্টি-স্পাইওয়্যার ব্যবহার করা, সফটওয়্যারের পাসওয়ার্ড আপডেট রাখা এবং ফায়ারওয়াল চালু রাখা;

(ঙ) সার্ভারে Biometric Authentication like Finger Print, Scans Option থাকলে তা Enable করে রাখা;

(চ) সার্ভারের অপ্রয়োজনীয় Service বন্ধ রাখা;

(ছ) সার্ভারে অননুমোদিত সফটওয়্যার ইনস্টল না করা;

(জ) পেনড্রাইভ, মোবাইল হার্ডডিস্ক, মেমরি কার্ড, সিডি/ডিভিডি ডিস্ক ইত্যাদি ভাইরাস স্ক্যান করে ব্যবহার করা;

(ঝ) লাইসেন্সকৃত আপডেটেড অপারেটিং সিস্টেম, এন্টিভাইরাস, এপ্লিকেশন সফটওয়্যার ইত্যাদি ব্যবহার করা;

(ঞ) ব্লু-টুথ, ওয়াই-ফাই, ইনফ্রারেড ইত্যাদি বন্ধ রাখা;

(ট) ডাটাবেইজের নিয়মিত ব্যাক-আপ নিশ্চিত করা;

(ঠ) সার্ভারে লগ ফাইল নিয়মিত পর্যবেক্ষণ করা;

(ড) অডিট লগ চালু রাখা;

(ঢ) যে কোন চলমান সিস্টেমের ব্যাকআপ সার্ভার প্রস্তুত রাখা;

(ণ) নিরাপত্তার বিষয়ে নিশ্চিত না হয়ে ফ্রি সফটওয়্যার ডাউনলোড করা থেকে বিরত থাকা;

(ত) সার্ভার নিয়মিত পরিষ্কার পরিচ্ছন্ন রাখা;

(থ) সার্ভারের physical security নিশ্চিত করা; এবং

(দ) প্রয়োজনে বাংলাদেশ কম্পিউটার কাউন্সিল কর্তৃক সার্ভারের হার্ডওয়্যারের কোয়ালিটি টেস্ট করা।

৫.১২. সামাজিক যোগাযোগ মাধ্যম সুরক্ষায় করণীয়:

(ক) সামাজিক যোগাযোগ মাধ্যম ব্যবহারের সময় সংশ্লিষ্ট ব্যক্তিবর্গের প্রোফাইল সম্পর্কে জানা ও সচেতন থাকা;

(খ) সামাজিক যোগাযোগ মাধ্যম যেমন: ফেসবুক, টুইটার, স্কাইপি, ইমো, ভাইবার, হোয়াটসঅ্যাপ ইত্যাদিতে কোন পোস্ট/আপলোড, কমেন্ট, লাইক, বন্ধু বাছাই, শেয়ার করার ক্ষেত্রে যথাযথ সতর্কতা অবলম্বন করা;

(গ) অসামাজিক কোন সাইটে (যেমন: পর্নোসাইট, জুয়া বা লটারি বিষয়ক সাইট, জঙ্গিবাদ বিষয়ক সাইট ইত্যাদি) প্রবেশ থেকে বিরত থাকা;

(ঘ) সামাজিক যোগাযোগ মাধ্যম ব্যবহারের ক্ষেত্রে সেটিংস থেকে লগইন নোটিফিকেশন অপশন চালু রাখা;

(ঙ) নিজের অ্যাকাউন্টে অতিরিক্ত আরেকটি ই-মেইল ঠিকানা বা মোবাইল নম্বর যোগ করা যাতে কোনোভাবে অ্যাকাউন্ট হ্যাক হলে পুনরুদ্ধার করা যায়;

(চ) সামাজিক যোগাযোগের বিভিন্ন মাধ্যমে সরকার বা রাষ্ট্রের ভাবমূর্তি ক্ষুণ্ন হয় এমন কোনো পোস্ট/আপলোড, কমেন্ট, লাইক, শেয়ার করা থেকে বিরত থাকা;

(ছ) সরকারি প্রতিষ্ঠানে সামাজিক যোগাযোগ মাধ্যম ব্যবহার সংক্রান্ত নির্দেশিকা, ২০১৯ (পরিমার্জিত সংস্করণ) অনুসরণ করা;

(জ) সাইন ইন করার ক্ষেত্রে 2-Factor Authentication-এর মাধ্যমে One-time Password (OTP) অপশন চালু রাখা; এবং

(ঝ) প্রয়োজনে অনলাইন অটো জিও টাইপিং ফিচার অপশন বন্ধ রাখা।

৬. ঝুঁকি ব্যবস্থাপনা:

৬.১ ঝুঁকি বিশ্লেষণ:

ডিজিটাল তথ্য সম্পদের ঝুঁকি বিশ্লেষণ অত্যন্ত গুরুত্বপূর্ণ। এ ক্ষেত্রে ঝুঁকির ক্ষেত্রসমূহ শনাক্ত করার পাশাপাশি তথ্য সম্পদ সুরক্ষার ক্ষেত্রে যে সকল সমস্যা/প্রতিবন্ধকতা থাকতে পারে তা যথাযথ বিশ্লেষণ করে প্রতিকারের উপায় চিহ্নিত করতে হবে। প্রতিষ্ঠানের কোথায়, কখন, কীভাবে কোন প্রকৃতির আকস্মিক ঘটনা ঘটতে পারে তা যথাযথভাবে বিশ্লেষণ করা দরকার যাতে তথ্য সম্পদে যে সকল আকস্মিক ঘটনা ঘটার সম্ভাবনা আছে বা ভবিষ্যতে ঘটতে পারে তার প্রতিটি বিষয় পুঙ্খানুপুঙ্খ শনাক্ত করে সে অনুযায়ী প্রয়োজনীয় পদক্ষেপ গ্রহণ করা যায়।

৬.২ ঝুঁকি মোকাবেলায় কর্মপরিকল্পনা প্রণয়ন:

ঝুঁকি প্রশমন করার জন্য ঝুঁকি বিশ্লেষণ অত্যন্ত গুরুত্বপূর্ণ। ঝুঁকি বিশ্লেষণের ফলাফলের ওপর ভিত্তি করেঝুঁকিসমূহকেকিভাবে প্রশমন করা যায় সে বিষয়ে সিদ্ধান্ত গ্রহণ করার জন্য ঝুঁকির ফলাফল ও ঝুঁকির মাত্রা বিবেচনা করে একটি সার্বিক কর্ম-পরিকল্পনা প্রণয়ন করতে হবে। এ কর্মপরিকল্পনায় বিভিন্ন পর্যায়ে থাকতে পারে। যেমন:

ক. ঘটনা ঘটার পূর্বে, প্রতিরোধমূলক ব্যবস্থা গ্রহণ;

খ. ঘটনা ঘটার সময়, ঝুঁকি শনাক্তকরণের মাধ্যমে ঝুঁকি অপসারণ;

গ. ঘটনা ঘটার পর, সংশোধনমূলক ব্যবস্থা গ্রহণ করে ঝুঁকি অপসারণ।

৬.৩ আকস্মিক ঘটনা ব্যবস্থাপনা:

তথ্য নিরাপত্তায় দূর্ঘটনা যে কোনো সময় ঘটতে পারে। এ বিষয়টি বিবেচনায় নিয়ে যথাযথ সতর্কতা অবলম্বন করা প্রয়োজন যাতে যে কোনো ধরনের প্রাকৃতিক দুর্যোগ যেমন-বন্যা, অগ্নিকান্ড, ভূমিকম্প ইত্যাদি ও সাইবার দূর্ঘটনার

Sheree2

সময় দাপ্তরিক কার্যক্রমের ধারাবাহিকতা রক্ষায় স্বল্প সময়ের মধ্যে তথ্য ব্যবস্থা পুনরুদ্ধার কার্যক্রম শুরু করা যায়। আকস্মিক ঘটনা মোকাবিলার জন্য সকল প্রতিষ্ঠানের একটি জরুরি সাড়া প্রদানকারী টিম গঠন করা প্রয়োজন। অনেক ক্ষেত্রে এ ধরনের পরিস্থিতি শুধুমাত্র প্রতিষ্ঠানের নিজস্ব জনবল দ্বারা মোকাবিলা করা সম্ভব হয় না। এ কারণে জরুরি সাড়া প্রদানকারী টিম গঠনের ক্ষেত্রে নিজস্ব জনবলের পাশাপাশি অন্যান্য বিশেষায়িত প্রতিষ্ঠানের সদস্যগণকেও অন্তর্ভুক্ত করা যেতে পারে। আকস্মিক ঘটনা মোকাবিলার জন্য এ টিমের কর্ম-পরিকল্পনা থাকতে হবে। বিশেষজ্ঞটিম ঘটনা ঘটার পরপরই তদন্তপূর্বক যথাযথ রিপোর্ট প্রদান করবে। আকস্মিক ঘটনা তদন্তের পর সংশ্লিষ্ট রেকর্ডসমূহ যথাযথভাবে সংরক্ষণ করতে হবে। অধিকন্তু এ রিপোর্ট প্রয়োজনীয়তার নিরিখে যথাযথ কার্যক্রম গ্রহণের নিমিত্ত উর্ধ্বতন কর্তৃপক্ষকে অবহিত করতে হবে।

৭. তথ্য ব্যবস্থাপনা নিরীক্ষা:

প্রতিষ্ঠানের তথ্য ব্যবস্থাপনা উন্নয়নসহ যে বিপর্যয় রোধ করার ক্ষেত্রে এর নিরীক্ষা অত্যন্ত গুরুত্বপূর্ণ। গুরুত্বপূর্ণ তথ্য ব্যবস্থাপনা অবকাঠামো পরিচালনার সাথে সংশ্লিষ্ট প্রতিষ্ঠানসমূহকে অবশ্যই সময়ে সময়ে তথ্য ব্যবস্থাপনা নিরীক্ষা করতে হবে। তথ্য ব্যবস্থাপনায় বিশেষায়িত নিরীক্ষা সংস্থার মাধ্যমে নিরীক্ষা পরিচালনা করার পাশাপাশি প্রতিষ্ঠানের অভ্যন্তরীণ বিশেষজ্ঞ জনবলের মাধ্যমেও নিয়মিত নিরীক্ষা কার্যক্রম পরিচালনা করতে হবে।

৮. পরিদর্শন:

ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য-উপাত্ত সংরক্ষণসহ এগুলোর রক্ষণাবেক্ষণ করার বিষয়টি নিয়মিত তদারকি করা অত্যন্ত জরুরি। উর্ধ্বতন কর্তৃপক্ষ কর্তৃক প্রতিষ্ঠানের ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য-উপাত্ত সংরক্ষণসহ এ সকল সম্পদের ব্যবস্থাপনার বিষয়টি নিয়মিত পরিদর্শন করতে হবে।

৯. প্রশিক্ষণ:

ডিজিটাল ডিভাইস, ইন্টারনেট ও তথ্য রক্ষণাবেক্ষণ এবং নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে প্রশিক্ষণের ব্যবস্থা গ্রহণ করতে হবে।

১০. তথ্য নিরাপত্তার আইনগত বিষয়সমূহ:

তথ্য নিরাপত্তার সাথে সংশ্লিষ্ট বিভিন্ন আইন ও বিধি-বিধান সম্পর্কে সচেতন থেকে সকলকে দায়িত্ব পালন করতে হবে। এ ক্ষেত্রে নিম্নোক্ত আইন, বিধি-বিধান, নীতিমালা ও গাইডলাইন ছাড়াও সংশ্লিষ্ট অন্যান্য আইন ওবিধি-বিধানের প্রতি লক্ষ্য রাখতে হবে:

১. দি পেটেন্ট অ্যান্ড ডিজাইন অ্যাক্ট, ১৯১১;

২. রেকর্ড ম্যানুয়াল, ১৯৪৩;

৩. জাতীয় আরকাইভ আইন, ১৯৮৩;

৪. কপিরাইট অ্যাক্ট, ২০০০ (২০০৫-এ সংশোধিত);

৫. তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬;

৬. তথ্য অধিকার আইন, ২০০৯;

৭. ক্রিপটোগ্রাফিক নিয়ন্ত্রণের জন্য PKI সম্পর্কিত বিধি, ২০১০;

৮. সচিবালয় নির্দেশমালা, ২০১৪;

Shereen

৯. বাংলাদেশ কম্পিউটার কাউন্সির কর্তৃক প্রণিত Government of Bangladesh Information Security Manual, 2016;

১০. তথ্য ও যোগাযোগ প্রযুক্তি নীতিমালা, ২০১৮;

১১. ডিজিটাল নিরাপত্তা আইন, ২০১৮;

১২. সরকারি চাকরি আইন-২০১৮;

১৩. সরকারি ই-মেইল নীতিমালা ২০১৮;

১৪. সরকারি প্রতিষ্ঠানে সামাজিক যোগাযোগ মাধ্যম ব্যবহার সংক্রান্ত নির্দেশিকা, ২০১৯ (পরিমার্জিত সংস্করণ);

১৫. সাইবার সিকিউরিটি স্ট্রাটেজি, ২০১৪; এবং

১৬. তথ্য নিরাপত্তা পলিসি গাইডলাইন, ২০১৪।

Sheroo