মন্ত্রিপরিষদ বিভাগের ডিজিটাল তথ্য নিরাপত্তা নির্দেশিকা, ২০১৭

মন্ত্রিপরিষদ বিভাগ
২৬ শ্রাবণ ১৪২৪/১০ আগস্ট ২০১৭

মন্ত্রিপরিষদ বিভাগের ডিজিটাল তথ্য নিরাপত্তা নির্দেশিকা, ২০১৭

মন্ত্রিপরিষদ বিভাগ

২৬ শ্রাবণ ১৪২৪/১০ আগস্ট ২০১৭

১. প্রেক্ষাপট:

বাংলাদেশকে ২০২১ সালের মধ্যে মধ্যম আয়ের দেশে এবং ২০৪১ সালের মধ্যে উন্নত দেশে উন্নীত করতে সরকার ব্যাপক উন্নয়ন কার্যক্রম গ্রহণ করেছে। সরকারের বহুমুখী এ সকল উন্নয়ন কার্যক্রম দ্রুত এবং সফল বাস্তবায়নের জন্য সকল সরকারি প্রতিষ্ঠানকে ই-গভর্নেন্স কাঠামোর আওতায় এনে 'ডিজিটাল বাংলাদেশ' গঠন করা প্রয়োজন। বর্তমানে সরকারের বিভিন্ন মন্ত্রণালয়/বিভাগ, অধিদপ্তর/সংস্থা ও তাদের আওতাধীন প্রতিষ্ঠানসমূহ ডিজিটাল বাংলাদেশ বাস্তবায়নে নানাবিধ কার্যক্রম পরিচালনা করছে। এ কার্যক্রমের অংশ হিসেবে দেশে ইতোমধ্যে উল্লেখযোগ্য সংখ্যক গুরুত্বপূর্ণ ডিজিটাল তথ্যভাণ্ডার প্রস্তুত হয়েছে। যেমন: জাতীয় তথ্য বাতায়ন, জন্ম ও মৃত্যু নিবন্ধন, জাতীয় পরিচয়পত্র, ই-ভূমি তথ্য ও সেবা কাঠামো, ই-নথি, ই-প্রকিউরমেন্ট, ই-ব্যাংকিং, ইএফটি, ই-ট্যাক্স, ই-টিকেটিং, জাতীয় ই-তথ্যকোষ, ই-বুক ইত্যাদি। এ সকল কার্যক্রমের প্রধান উদ্দেশ্য সরকারি সেবা সহজিকরণ এবং সরকারের বিভিন্ন উন্নয়নমূলক কার্যক্রম বাস্তবায়নে সক্ষমতা বৃদ্ধি। এ জন্য প্রতিষ্ঠানের সব ধরনের তথ্য যেমন ডিজিটাইজড করা প্রয়োজন তেমনি এ তথ্য এমনভাবে প্রক্রিয়া ও সংরক্ষণ করতে হবে যাতে তা হারিয়ে না যায় কিংবা এর কোনরূপ অপব্যবহার না হয়। বর্তমানে বিশ্বব্যাপী ই-গভর্নেন্স কার্যক্রমের পরিধি ব্যাপকভাবে বৃদ্ধি পাওয়ার কারণে সামগ্রিক অর্থনৈতিক উন্নয়ন তথা জাতীয় সমৃদ্ধির ক্ষেত্রে ডিজিটাল তথ্য যথাযথভাবে সংরক্ষণ ও ব্যবহারের গুরুত্ব অপরিসীম।

ডিজিটাল তথ্য যথাযথভাবে সংরক্ষণ ও ব্যবহারের ক্ষেত্রে বর্তমানে সাইবার আক্রমণ অন্তরায় হিসেবে দেখা দিচ্ছে। তথ্য সুরক্ষা বিষয়ক সক্ষমতার অভাব, দুর্বল ও অব্যবস্থাপনাজনিত নিরাপত্তা নিয়ন্ত্রণ, বিশেষায়িত জ্ঞান ও দক্ষ জনবলের অভাবসহ নানাবিধ কারণে বিভিন্ন প্রতিষ্ঠান তথ্য বিপর্যয়, তথ্য চুরি, ডিসট্রিবিউটেড ডিনাইয়াল অব সার্ভিস ইত্যাদির মাধ্যমে সাইবার আক্রমণের শিকার হচ্ছে। এ সব আক্রমণ হতে ডিজিটাইজড তথ্য সম্পদ সুরক্ষায় পর্যাপ্ত প্রশাসনিক নিরাপত্তামূলক ব্যবস্থা গ্রহণ করা প্রয়োজন। প্রতিষ্ঠানের ডিজিটাইজড তথ্যসম্পদ সুরক্ষায় তথ্য নিরাপত্তা নির্দেশিকা গুরুত্বপূর্ণ ভূমিকা রাখতে পারে।

২. ভূমিকা:

তথ্য একটি প্রতিষ্ঠানের সর্বাধিক মূল্যবান সম্পদ। এ কারণে তথ্য সংরক্ষণ ও ব্যবহারের ক্ষেত্রে যথাযথ সতর্কতা অবলম্বন করা প্রয়োজন। প্রবেশাধিকার বিবেচনায় তথ্যের বিভিন্ন প্রকারভেদ রয়েছে। যেমন: কিছু তথ্য উন্মুক্ত, কিছু তথ্য গোপনীয় এবং কিছু তথ্য অতি গোপনীয়। উন্মুক্ত তথ্য যে কোন ব্যক্তি বা প্রতিষ্ঠান তথ্যভাণ্ডার থেকে গ্রহণ করে ব্যবহার করতে পারেন। আবার গোপনীয় ও অতি গোপনীয় তথ্য প্রতিষ্ঠানের নির্দিষ্ট কিছু ব্যক্তি ব্যবহার করতে পারেন। সুতরাং এক্ষেত্রে একটি প্রতিষ্ঠানের তথ্য এবং এ তথ্যে প্রবেশাধিকার সম্পর্কে স্বচ্ছ ধারণা থাকা প্রয়োজন। বর্তমান বিশ্বে সকলের জন্য তথ্যের উন্মুক্ত ক্ষেত্র হল ইন্টারনেট। ইন্টারনেট, লোকাল এরিয়া নেটওয়ার্ক (LAN) ও অন্যান্য প্রযুক্তি যেমন: কম্পিউটার, সার্ভার, ল্যাপটপ, মোবাইল ফোন, সামাজিক যোগাযোগ মাধ্যম, বেতার, টেলিভিশন ইত্যাদি তথ্যকে সহজলভ্য ও সাশ্রয়ী করেছে। তবে তথ্যের এ সহজলভ্যতা দেশের অভ্যন্তরে আইন-শৃঙ্খলা বিঘ্নের অন্যতম

হাতিয়ার হিসেবেও ব্যবহার হতে পারে। তাই তথ্য ব্যবহারের ক্ষেত্রে সকলেরই দায়িত্বশীল ভূমিকা পালন করা প্রয়োজন। ডিজিটাল তথ্য ব্যবস্থায় এ সকল তথ্য সংরক্ষণ ও সুষ্ঠুভাবে ব্যবহারের জন্য 'মন্ত্রিপরিষদ বিভাগের ডিজিটাল তথ্য নিরাপত্তা নির্দেশিকা, ২০১৭' প্রণয়ন করা হল। এ নির্দেশিকা ব্যবহার করে তথ্য ব্যবস্থার সঙ্গে সংশ্লিষ্ট কর্মকর্তা-কর্মচারীগণ তথ্যের নিরাপত্তায় আরও দায়িত্বশীল ভূমিকা রাখতে সক্ষম হবেন।

৩. এ নির্দেশিকায় যা অন্তর্ভুক্ত করা হয়েছে:

১. তথ্য নিরাপত্তা সংক্রান্ত কতিপয় বিষয়সমূহের সংক্ষিপ্ত পরিচিতি;
২. উদ্দেশ্য;
৩. নির্দেশিকার পরিধি;
৪. তথ্যসম্পদ ব্যবস্থাপনা;
৫. তথ্য সত্ত্বাধিকারী এবং তথ্য সংরক্ষকের দায়িত্ব;
৬. তথ্য নিরাপত্তা কৌশলসমূহ;
৭. তথ্য নিরাপত্তার আইনগত বিষয়সমূহ;
৮. ঝুঁকি ব্যবস্থাপনা;
৯. তথ্য নিরাপত্তা সম্পর্কিত প্রশিক্ষণ;
১০. তথ্য ব্যবস্থা নিরীক্ষা ও প্রত্যয়ন;
১১. আকস্মিক ঘটনা ব্যবস্থাপনা;
১২. তথ্য নিরাপত্তা প্রতিষ্ঠায় অনুসৃত মানদণ্ড; এবং
১৩. বাস্তবায়ন, পরিবীক্ষণ ও মূল্যায়ন।

৩.১ তথ্য নিরাপত্তা সংক্রান্ত কতিপয় বিষয়সমূহের সংক্ষিপ্ত পরিচিতি:

(১) "আক্রমণ" অর্থ কোন তথ্যসম্পদ ক্ষতি, বিনাশ, ধ্বংস, উন্মুক্ত, পরিবর্তন, অকেজো, চুরি অথবা অননুমোদিত প্রবেশ বা অননুমোদিতভাবে নিয়ন্ত্রণ করার প্রচেষ্টা;
(২) "উপাত্ত দূষণ" অর্থ এমন কোন প্রোগ্রাম যা কোন ডিজিটাল ডিভাইস বা কম্পিউটার সিস্টেম বা নেটওয়ার্কে রক্ষিত কোন রেকর্ড, উপাত্ত বা সঞ্চালন কার্যের ক্ষতি, পরিবর্তন অথবা স্বাভাবিক কার্যক্রমকে বাধাগ্রস্ত করে;
(৩) "গোপনীয়" অর্থ এমন কোন বিষয় যা অননুমোদিত কোন ব্যক্তি বা সত্ত্বার নিকট কোন ব্যবস্থা বা প্রক্রিয়ায় প্রদান বা প্রকাশ করা যাবে না;
(৪) "ঝুঁকি বিশ্লেষণ" অর্থ ঝুঁকির উৎস শনাক্তকরণ ও ঝুঁকির পরিমাণ নির্ণয় করা;
(৫) "ঝুঁকি মূল্যায়ন" ঝুঁকির মাপকাঠির সঙ্গে পরিমাপকৃত ঝুঁকির তুলনা করে ঝুঁকির মাত্রা নির্ধারণ;
(৬) "ঝুঁকি ব্যবস্থাপনা" অর্থ ঝুঁকি সম্পর্কে প্রয়োজনীয় নির্দেশনা প্রদান ও ঝুঁকি নিয়ন্ত্রণ করার সমন্বিত কর্মতৎপরতা;

(৭) "ঝুঁকি নিরসন" অর্থ ঝুঁকি নিয়ন্ত্রণ বা হ্রাস করার ব্যবস্থা নির্ধারণ ও বাস্তবায়ন প্রক্রিয়া;
(৮) "ঝুঁকি নির্ধারণ" অর্থ ঝুঁকি বিশ্লেষণ ও মূল্যায়নের সামগ্রিক প্রক্রিয়া;
(৯) "ডিজিটাল ডিভাইস" অর্থ যে কোন ইলেকট্রনিক, ডিজিটাল, ম্যাগনেটিক, অপটিক্যাল বা তথ্য প্রক্রিয়াকরণ যন্ত্র বা সিস্টেম যা ব্যবহার করে যৌক্তিক, গাণিতিক এবং স্মৃতি বিষয়ক কার্যক্রম সম্পন্ন করা যায়। কোন ডিজিটাল সিস্টেম বা নেটওয়ার্কের সঙ্গে সংযুক্ত এবং যাতে সকল ইনপুট, আউটপুট, প্রক্রিয়াকরণ, সঞ্চিত, যোগাযোগ ইত্যাদি সুবিধা প্রদান করে এমন বিষয়সমূহও এর অন্তর্ভুক্ত হবে;
(১০) "তথ্য ব্যবস্থা" অর্থ তথ্যপ্রযুক্তি ব্যবহারের মাধ্যমে ইলেকট্রনিক উপায়ে উপাত্ত প্রক্রিয়াকরণের ইলেকট্রনিক ব্যবস্থা যার মধ্যে কম্পিউটার সিস্টেম, সার্ভার, ওয়ার্কস্টেশন, টার্মিনাল, স্টোরেজ মিডিয়া, কমিউনিকেশন ডিভাইস, নেটওয়ার্ক রিসোর্স, ইন্টারনেট ইত্যাদি অন্তর্ভুক্ত রয়েছে;
(১১) "তথ্য সংরক্ষণ" অর্থ কম্পিউটার, সার্ভার, অপটিক্যাল ডিস্ক বা স্টোরেজ মাধ্যম, ক্লাউড ইত্যাদিতে তথ্য সংরক্ষণ করার ব্যবস্থা;
(১২) "তথ্য নিরাপত্তা" অর্থ তথ্যের গোপনীয়তা, শুদ্ধতা ও লভ্যতা সংরক্ষণ;
(১৩) "তথ্য সংরক্ষণের ঝুঁকি" অর্থ দাপ্তরিক কাজে ব্যবহৃত সকল কম্পিউটার/সার্ভার/ল্যাপটপ/ট্যাব ইত্যাদির মাধ্যমে সংরক্ষিত তথ্যে বিভিন্ন ধরনের ভাইরাস, ম্যালওয়্যার ও স্প্যাম আক্রমণে তথ্য নষ্ট/হারিয়ে যাওয়ার সম্ভাবনা থাকে বা ক্লাউডে সংরক্ষিত তথ্য হ্যাকিং-এর মাধ্যমে নিয়ন্ত্রণে নেওয়ার সম্ভাবনা থাকে এরূপ অবস্থা;
(১৪) "তথ্য নিরাপত্তায় আকস্মিক ঘটনা" অর্থ এক বা একাধিক অনাকাঙ্ক্ষিত বা অপ্রত্যাশিত ঘটনা যা তথ্য নিরাপত্তায় প্রতিষ্ঠানের কার্যক্রম ব্যাহত হয় বা তথ্য নিরাপত্তায় হুমকি হিসেবে পরিগণিত হতে পারে;
(১৫) "তথ্য নিরীক্ষা" অর্থ তথ্য যথাযথভাবে সংরক্ষণ করা হয়েছে কিনা তা পর্যবেক্ষণ এবং মূল্যায়ন;
(১৬) "তথ্যসম্পদ" অর্থ প্রতিষ্ঠানের নিকট মূল্য রয়েছে এমন তথ্য সংশ্লিষ্ট বিষয়সমূহ;
(১৭) "পাসওয়ার্ড" অর্থ এমন এক ধরনের উপাত্ত বা ডাটা যার মাধ্যমে কম্পিউটার বা ডিজিটাল ডিভাইস, সার্ভিস বা সিস্টেমে ব্যবহার ও প্রবেশাধিকার লাভ করা যায়;
(১৮) "ভাইরাস" অর্থ এক ধরনের প্রোগ্রাম, যা কোন কম্পিউটার বা ডিজিটাল ডিভাইস কর্তৃক সম্পাদিত কার্যকে বিনাশ, ক্ষতি বা এর কার্যসম্পাদনের দক্ষতায় বিরূপ প্রভাব বিস্তার করে;
(১৯) "নিয়ন্ত্রণ" অর্থ প্রশাসনিক, কারিগরি, ব্যবস্থাপনা বিষয়ক, কিংবা আইন সংক্রান্ত পলিসি, পদ্ধতি, নির্দেশনা, অনুশীলন বা সাংগঠনিক কাঠামোসহ ঝুঁকি ব্যবস্থাপনাকে বুঝাবে; এবং
(২০) "সামাজিক যোগাযোগ মাধ্যম" অর্থ কম্পিউটার বা ডিজিটাল ডিভাইস ব্যবহারের মাধ্যমে অফলাইন বা অনলাইনে পারস্পরিক যোগাযোগ, তথ্য-উপাত্ত আদান-প্রদান, চ্যাট, ভিডিও-চ্যাট, ই-মেইল, গ্রুপ বা ব্লগ-সাইট ইত্যাদি।

৩.২ উদ্দেশ্য:

কোন প্রতিষ্ঠানের অত্যন্ত গুরুত্বপূর্ণ এবং স্পর্শকাতর সম্পদ হল তথ্যসম্পদ। এ সম্পদের সুষ্ঠু ব্যবহার একদিকে যেমন দেশের সমৃদ্ধি এবং উন্নয়নের জন্য অপরিহার্য অন্যদিকে এ সম্পদের অপব্যবহার রোধ করা রাষ্ট্রীয় নিরাপত্তা তথা আইন-শৃঙ্খলা পরিস্থিতি স্বাভাবিক রাখার জন্যও অত্যন্ত গুরুত্বপূর্ণ। সরকারি ও বেসরকারি দপ্তর/সংস্থা/প্রতিষ্ঠানসমূহ তার জনবল ও প্রযুক্তির মাধ্যমে ডিজিটাল তথ্যের সংরক্ষণ করে থাকে।

সার্বিকভাবে এ নির্দেশিকা প্রণয়নের উদ্দেশ্য:

(১) তথ্য সম্পর্কে ধারণা, সংরক্ষণ এবং নিরাপত্তা বিষয়ে প্রাতিষ্ঠানিক সচেতনতা গড়ে তোলা;
(২) প্রশিক্ষণ প্রদানের মাধ্যমে তথ্য নিরাপত্তার বিষয়ে সংশ্লিষ্ট সকলকে দক্ষ করে গড়ে তোলা; এবং
(৩) তথ্যকে বাইরের আক্রমণ, হুমকি, অপব্যবহার, ক্ষতি, বিনাশ অথবা তথ্যে অননুমোদিত প্রবেশাধিকার রোধে কৌশল নির্ধারণ।

৩.৩ নির্দেশিকার পরিধি:

মন্ত্রিপরিষদ বিভাগের ডিজিটাল তথ্যের নিরাপত্তা নিশ্চিত করার জন্য এ নির্দেশিকা প্রণয়ন করা হয়েছে। এ বিভাগের তথ্য সুরক্ষাসহ সংশ্লিষ্ট বিষয়ে পলিসি প্রণয়নে সরকারি বিভিন্ন আইন, বিধিমালা, প্রজ্ঞাপন, পরিপত্র, নির্দেশনা ইত্যাদির সহায়ক দলিল হিসেবে এ নির্দেশিকা ব্যবহৃত হবে। অন্যান্য সরকারি প্রতিষ্ঠানসমূহ প্রয়োজনে এ নির্দেশিকা বা এর কোন বিষয় অনুসরণ করতে পারবে।

৩.৪ তথ্য সম্পদ ব্যবস্থাপনা:

ক. তথ্যসম্পদ:

কোন প্রতিষ্ঠানের গুরুত্বপূর্ণ তথ্য বা উপাত্ত সম্পর্কে সংশ্লিষ্ট সকলের স্পষ্ট ধারণা থাকা প্রয়োজন। তথ্যের অবস্থান নিরূপণ, তথ্যসম্পদের মালিকানা, তত্ত্বাবধায়ক নির্ধারণ এবং তথ্য কীভাবে সংরক্ষণ করতে হবে সে বিষয়সমূহ প্রতিষ্ঠানের সংশ্লিষ্ট সকলের জানতে হবে।

সাধারণত প্রতিষ্ঠানে যে সকল তথ্য সংরক্ষণ করা হয় তা একদিকে যেমন প্রশাসনিক কাজে গুরুত্বপূর্ণ অন্যদিকে রাজনৈতিক, বাণিজ্যিক কিংবা ব্যক্তিগত ব্যবহারের ক্ষেত্রেও গুরুত্বপূর্ণ। তথ্যসম্পদ বিভিন্নরূপ হতে পারে যেমন:

১. প্রামাণ্য দলিল ও নথিপত্র;
২. ইলেকট্রনিক উপাত্ত;
৩. তথ্য ব্যবস্থাপনাসমূহ (সফট্ওয়্যার, হার্ডওয়্যার ও নেটওয়ার্ক) যার মাধ্যমে তথ্য সংরক্ষণ, প্রক্রিয়াকরণ ও আদান-প্রদান করা হয়;
৪. ব্যক্তির বুদ্ধিবৃত্তিক তথ্য (জ্ঞান বা ধারণাসমূহ);
৫. ভৌত উপকরণসমূহ যা তথ্যের ডিজাইন, উপাদান বা ব্যবহারের সঙ্গে সংশ্লিষ্ট; এবং
৬. ছবি, অডিও বা ভিডিও ক্লিপ ইত্যাদি।

খ. তথ্যসম্পদের শ্রেণিকরণ:

তথ্য যথাযথভাবে সংরক্ষণ এবং তথ্যভাণ্ডারে অনধিকার প্রবেশ রোধে তথ্যের শ্রেণিকরণ করা প্রয়োজন। তথ্যের শ্রেণিকরণের ক্ষেত্রে তথ্যের প্রয়োজনীয়তা, অগ্রাধিকার ও তথ্য ব্যবহারে প্রত্যাশিত সুরক্ষা প্রদানের বিষয় বিবেচনা করা প্রয়োজন। বিভিন্ন প্রতিষ্ঠানের তথ্যের স্পর্শকাতরতা ও গুরুত্বের ভিন্ন ভিন্ন মাত্রা রয়েছে। কিছু কিছু তথ্য অধিকমাত্রায় সুরক্ষা বা নিয়ন্ত্রণ করা প্রয়োজন হতে পারে। সে জন্য তথ্যের নিরাপত্তা স্তর নির্ধারণ এবং সে অনুযায়ী সতর্কতার সঙ্গে ব্যবহারের প্রয়োজনীয়তার বিষয়ে লক্ষ্য রেখে তথ্যের শ্রেণিকরণ করা সমীচীন। সকল তথ্য আবার সকল প্রতিষ্ঠানের নিকট সমান গুরুত্বপূর্ণ নাও হতে পারে। তথ্যের গোপনীয়তা অনেক সময় স্থান, কাল এবং ব্যক্তি বা প্রতিষ্ঠানভেদে একইরূপ নাও হতে পারে। তথ্যের শ্রেণিকরণে তথ্যসম্পদের গোপনীয়তা, শুদ্ধতা, প্রামাণ্যতা ও সহজলভ্যতা-এ বিষয়সমূহের গুরুত্ব অপরিসীম। বিভিন্ন প্রতিষ্ঠানে তথ্যের মূল্যমান, আইনগত প্রয়োজন, গোপনীয়তা, স্পর্শকাতরতা ও গুরুত্ব বিবেচনায় তথ্যকে নিম্নোক্তভাবে শ্রেণিকরণ করা হয়ে থাকে:

১. অতি গোপনীয়
২. বিশেষ গোপনীয়
৩. গোপনীয়
৪. সীমিত
৫. উন্মুক্ত

যে কোন প্রতিষ্ঠানের তথ্য শ্রেণিকরণের ক্ষেত্রে এ সকল বিষয়সমূহ বিবেচনা করে তথ্যের শ্রেণিকরণ করা প্রয়োজন। ফলে প্রতিষ্ঠানের সংশ্লিষ্ট দায়িত্ববান ব্যক্তিবর্গ তাদের প্রয়োজনে তথ্য সংগ্রহ, বিশ্লেষণ ও সংশ্লেষণপূর্বক তথ্যের যথাযথ ও যথার্থ নিরাপত্তা বিধানকল্পে এ সম্পদের সুষ্ঠু ব্যবস্থাপনা নিশ্চিত করতে পারেন।

গ. তথ্যসম্পদের ইনভেন্টরি:

সুষ্ঠু তথ্য ব্যবস্থাপনার জন্য প্রতিষ্ঠানের তথ্যসম্পদকে প্রথমে শনাক্ত করা সমীচীন। অতঃপর তথ্যসম্পদের একটি ইনভেন্টরি প্রস্তুত করা প্রয়োজন। ইনভেন্টরি প্রস্তুত করার সময় শনাক্তকৃত সকল তথ্যসম্পদের গুরুত্ব বিবেচনায় এনে তালিকাভূক্ত করতে হবে। তথ্যসম্পদের ইনভেন্টরিতে সম্পদের ধরন, আকার, অবস্থান, ব্যাকআপ, লাইসেন্স বিষয়ক তথ্য, প্রতিষ্ঠানের কাছে এর প্রয়োজনীয়তা এবং মূল্যসহ অন্যান্য প্রয়োজনীয় সকল তথ্য অন্তর্ভুক্ত রাখা প্রয়োজন।

ঘ. তথ্য শনাক্তকরণ চিহ্ন ও ব্যবহার:

যে কোন প্রতিষ্ঠান কর্তৃক তথ্য শ্রেণিকরণ পদ্ধতি অনুসরণে তথ্য শনাক্তকরণ ও ব্যবহারের জন্য একটি উপযুক্ত পদ্ধতি উন্নয়ন ও বাস্তবায়ন করা প্রয়োজন। এ পদ্ধতির মধ্যে ভৌত ও ইলেকট্রনিক আকারে বিদ্যমান তথ্যসমূহ শনাক্তকরণের ব্যবস্থা অন্তর্ভুক্ত করা সমীচীন।

৩.৫ তথ্য সত্ত্বাধিকারী এবং তথ্য সংরক্ষকের দায়িত্বঃ

যে কোন প্রতিষ্ঠানের তথ্যসম্পদ সুষ্ঠু ব্যবস্থাপনার লক্ষ্যে প্রতিষ্ঠানে যে সকল কর্মকর্তা-কর্মচারী তথ্যসম্পদ সংরক্ষণ, নিয়ন্ত্রণ এবং পরিচালনা সংক্রান্ত কার্যক্রমের সঙ্গে সংশ্লিষ্ট তাদের সকলেরই একক এবং যৌথভাবে দায়-দায়িত্ব রয়েছে। তবুও প্রতিষ্ঠানকে এ তথ্যসম্পদের যথাযথ সংরক্ষণ এবং নিরাপত্তা বিধানে যথাযথ কার্যকর পদক্ষেপ গ্রহণ করা প্রয়োজন। এ জন্য প্রতিষ্ঠানের তথ্যসম্পদের বিবরণসহ সংশ্লিষ্ট তথ্যসম্পদ সংরক্ষণ ও নিরাপত্তার জন্য কে কীভাবে দায়িত্ব পালন করবে সে বিষয়টি নির্ধারণ করা প্রয়োজন। তথ্যসম্পদ রক্ষণাবেক্ষণে একক বা যৌথভাবে দায়িত্বপালনকারী এ সকল ব্যক্তি বা সত্ত্বা সংশ্লিষ্ট প্রতিষ্ঠানের পক্ষে তথ্যসম্পদ রক্ষণাবেক্ষণের সত্ত্বাধিকারী হবেন। তথ্যসম্পদ রক্ষণাবেক্ষণের সত্ত্বাধিকারীকে তথ্যের শ্রেণিকরণ এবং সময়ে সময়ে তথ্যসমূহ পরীক্ষা-নিরীক্ষা করাসহ হালনাগাদ করা হয়েছে কি না বা তথ্য যথাযথ পর্যায়ের নিরাপত্তা নিয়ন্ত্রণের ভেতর রয়েছে কি না সে বিষয়টি নিশ্চিত করতে হবে। এ ক্ষেত্রে দাপ্তরিক প্রয়োজনে সত্ত্বাধিকারীর বিকল্প দায়িত্বপ্রাপ্ত কর্মকর্তা নির্ধারণ করা যেতে পারে। তথ্যসম্পদ সুরক্ষায় এ বিকল্প দায়িত্বপ্রাপ্ত কর্মকর্তা মূল দায়িত্বপ্রাপ্ত কর্মকর্তার অবর্তমানে দায়িত্ব পালন করবেন।

৩.৬ তথ্য নিরাপত্তার কৌশলসমূহঃ

তথ্য নিরাপত্তা কৌশল প্রণয়নের নিমিত্ত জনবল, প্রযুক্তি, পদ্ধতিসমূহের সমন্বয়ে কর্মপরিকল্পনা গ্রহণ করতে হবে। তথ্য নিরাপত্তা সম্পর্কিত নতুন নতুন হুমকি/ঝুঁকি নিরসনের লক্ষ্যে নিয়মিত প্রতিষ্ঠানের গৃহীত কৌশলসমূহ পুনঃনিরীক্ষা করে দেখতে হবে। তথ্য নিরাপত্তা কৌশলের বিষয়ে সর্বোত্তম পদ্ধতিসমূহ সম্পর্কে ধারণা নিয়ে প্রতিষ্ঠানের প্রয়োজন অনুযায়ী অনুশীলনযোগ্য টেকসই পদ্ধতি গ্রহণ করে তথ্য নিরাপত্তা কৌশল প্রণয়ন করা প্রয়োজন। উল্লেখ্য, আইএসও/আইইসি-২৭০০২ অনুযায়ী তথ্য নিরাপত্তা নিয়ন্ত্রণে জনবলের নিরাপত্তা, যন্ত্রপাতির নিয়ন্ত্রণ, প্রবেশাধিকার নিয়ন্ত্রণ, ভৌত ও পরিবেশগত নিরাপত্তা ব্যবস্থা, সফট্ওয়্যারের নিরাপত্তা, ব্যাকআপ ব্যবস্থা, নেটওয়ার্কের নিরাপত্তা ব্যবস্থাপনা, ক্রিপ্টোগ্রাফিক নিয়ন্ত্রণ, সঠিক প্রক্রিয়াকরণ, সিস্টেমের নিরাপত্তা ইত্যাদি বিষয়সমূহ গুরুত্বের সঙ্গে বিবেচনা করা হয়। এ ছাড়া, হার্ডওয়্যার, সফট্ওয়্যার, নেটওয়ার্ক বা অন্য কোন তথ্য পদ্ধতির সেবা গ্রহণ করার পূর্বে প্রতিষ্ঠানকে Service Level Agreement-এর বিষয়টিও বিবেচনা করা প্রয়োজন। সার্বিকভাবে এ বিভাগের তথ্য নিরাপত্তায় নিম্নোক্ত কৌশলসমূহ অনুসরণ করা যেতে পারে।

৩.৬.১ কম্পিউটার সুরক্ষায় করণীয়ঃ

ক) ডাটা সুরক্ষার জন্য কম্পিউটারের সঙ্গে ইউপিএস-এর ব্যবহার নিশ্চিত করা;

খ) কম্পিউটার/সার্ভার/ল্যাপটপ/ট্যাব/মোবাইল অবশ্যই পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;

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

ঘ) কম্পিউটারে সংরক্ষিত গুরুত্বপূর্ণ ফাইলসমূহ zip করে ব্যকআপ রাখা;

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

চ) কম্পিউটার/সার্ভার/ল্যাপটপ-কে ভাইরাস মুক্ত রাখার জন্য লাইসেন্স-ভার্সন এন্টিভাইরাস সফট্ওয়্যার ব্যবহার করা এবং সফট্ওয়্যার প্যাচ আপডেট রাখা;

ছ) ল্যাপটপ/ট্যাবে Biometric Authentication like Fingerprint, Scan Options থাকলে তা Enable করে রাখা;
জ) সার্ভার/কম্পিউটার/ল্যাপটপের অপ্রয়োজনীয় Service Status বন্ধ রাখা;
ঝ) সার্ভার/ডেস্কটপ/ল্যাপটপ/ট্যাবে অননুমোদিত সফট্ওয়্যার ইনস্টল না করা;
ঞ) সার্ভার/ডেস্কটপ/ল্যাপটপ/ট্যাব অপরিচিত কোন ব্যক্তির কাছে ছেড়ে না দেয়া;
ট) পেনড্রাইভ, মোবাইল হার্ডডিস্ক, মেমোরি কার্ড ইত্যাদি ভাইরাস স্ক্যান করে ব্যবহার করা;
ঠ) গুরুত্বপূর্ণ ডকুমেন্টসমূহ পাসওয়ার্ড দ্বারা সুরক্ষিত রাখা;
ড) লাইসেন্সকৃত আপডেটেড অপারেটিং সিস্টেম, এন্টিভাইরাস, এপ্লিকেশন সফট্ওয়্যার ইত্যাদি ব্যবহার করা;
ঢ) ব্যবহারের প্রয়োজন না হলে ব্লুটুথ, ওয়াই-ফাই, ইনফ্রারেড ইত্যাদি বন্ধ রাখা;
ণ) ডাটাবেইজ-এর নিয়মিত ব্যাকআপ রাখা;
ত) সার্ভারে লগ ফাইল নিয়মিত পর্যবেক্ষণ করা;
থ) যে কোন চলমান সিস্টেমের ব্যাকআপ সার্ভার প্রস্তুত রাখা;
দ) নিরাপত্তার বিষয়ে নিশ্চিত না হয়ে ফ্রি সফট্ওয়্যার ডাউনলোড করা থেকে বিরত থাকা;
ধ) নিয়মিত ডেস্কটপ/সার্ভার/ল্যাপটপ/ট্যাবকে ধূলাবালি থেকে সুরক্ষিত রাখা;
ন) সিস্টেম অ্যাডমিনের অনুমতি ব্যতীত দাপ্তরিক কম্পিউটারে কোন সফট্ওয়্যার ইনস্টল না করা;
প) কম্পিউটার/সার্ভার/ল্যাপটপ/ট্যাবের Physical Security নিশ্চিত করা;
ফ) কম্পিউটার মেঝেতে স্থাপন না করা এবং জানালার সন্নিকটে না রাখা; এবং
ব) কম্পিউটারে কাজ শেষ হওয়া মাত্র Shut down কমান্ড দিয়ে বন্ধ করা।

৩.৬.২ সফট্ওয়্যারের নিরাপত্তায় করণীয়:

ক) সফট্ওয়্যার প্রস্তুতের সময় ব্যবহৃত সকল টুলস হালনাগাদ আছে কি না তা যাচাই করা;
খ) সফট্ওয়্যার প্রস্তুতের সময় সংশ্লিষ্ট ফ্রেমওয়ার্কের আর্কিটেকচার যথাযথভাবে অনুসরণ করা;
গ) সার্ভারে ইউজার পাসওয়ার্ড এনক্রিপ্ট করে রাখা;
ঘ) ওয়েব এপ্লিকেশন নিরাপত্তার জন্য HTTPS প্রটোকল ব্যবহার করা;
ঙ) সফট্ওয়্যার ইনস্টলের পূর্বে আবশ্যিকভাবে নিরাপত্তা পরীক্ষণের ব্যবস্থাকরণ; এবং
চ) সফট্ওয়্যারের Vulnerability নিয়মিত পরীক্ষা করা এবং প্রাপ্ত ফলাফলের ভিত্তিতে প্রয়োজনীয় পদক্ষেপ নেয়া।

৩.৬.৩ 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 কনফিগার ও রিকভারি করার সময় সিকিউরিটি চেকের ব্যবস্থা রাখা;

গ) অন্য কোন ব্যক্তির সঙ্গে ব্যবহৃত পাসওয়ার্ডটি শেয়ার না করা এবং কোথাও লিখে না রাখা;
ঘ) পাসওয়ার্ড প্রস্তুতে নিজের নাম, জন্ম তারিখ, ব্যাংক অ্যাকাউন্ট নম্বর, স্ত্রী অথবা সন্তানের নাম ও জন্ম তারিখ, বিবাহ বার্ষিকীর তারিখ ইত্যাদি সচরাচর ব্যবহৃত বিষয়সমূহ ব্যবহারে বিরত থাকা;
ঙ) নিয়মিত (অন্তত ২/৩ মাস পর পর) পাসওয়ার্ড পরিবর্তন করা; এবং
চ) পাসওয়ার্ড পরিবর্তনের জন্য সিস্টেমে স্বয়ংক্রিয় সতর্কবার্তা প্রদর্শন করার ব্যবস্থা রাখা।

৩.৬.৪ লোকাল এরিয়া নেটওয়ার্ক (LAN) সুরক্ষায় করণীয়:

ক) LAN-এ অননুমোদিত ব্যক্তির ল্যাপটপ, ডেস্কটপ, ট্যাব ইত্যাদি ব্যবহার নিয়ন্ত্রণ করা;
খ) নেটওয়ার্ক সুরক্ষার জন্য ম্যনেজেবল সুইচ, ফায়ারওয়্যাল, রাউটার ইত্যাদি ব্যবহার করা;
গ) সার্ভার/কম্পিউটার/ল্যাপটপে রিমোট অ্যাকসেস নিয়ন্ত্রণ করা; এবং
ঘ) সার্ভার/কম্পিউটার/ল্যাপটপের কোন ড্রাইভ, ফোল্ডার, ফাইল ইত্যাদি অপরিচিত কারও সঙ্গে শেয়ার না করা।

৩.৬.৫ ইন্টারনেট ব্যবস্থাপনায় করণীয়:

ক) নিরাপদ গেটওয়ে ব্যতীত ইন্টারনেটের সংযোগ না নেওয়া;
খ) ইন্টারনেটে প্রয়োজনীয় ব্যান্ডউইথ নিশ্চিত করা;
গ) যথাযথ ব্যবস্থাপনার মাধ্যমে ইন্টারনেট ব্যান্ডউইথের সর্বোচ্চ ব্যবহার নিশ্চিত করা;
ঘ) ইন্টারনেট ব্যবহারের ক্ষেত্রে সংশ্লিষ্ট ডিভাইসের পরিচিতি নিশ্চিত করা;
ঙ) ব্যক্তিগত প্রয়োজনে প্রতিষ্ঠানের ইন্টারনেট ব্যবহার করা থেকে বিরত রাখা;
চ) ব্রাউজারে পাসওয়ার্ড স্থায়ীভাবে সংরক্ষণ না করা; এবং
ছ) নিয়মিত ব্রাউজার আপডেট রাখা।

৩.৬.৬ ই-মেইল ব্যবস্থাপনায় করণীয়:

ক) দাপ্তরিক কাজে সরকারি ই-মেইল ব্যবহার নিশ্চিত করা;
খ) নিয়মিত ই-মেইলের পাসওয়ার্ড পরিবর্তন করা;
গ) ই-মেইলে ব্যবহৃত পাসওয়ার্ড অন্য কারও সঙ্গে শেয়ার না করা;
ঘ) ই-মেইলের পাসওয়ার্ড কোথাও লিখে না রাখা;
ঙ) ই-মেইল ব্যবহার শেষে লগ আউট হওয়া;
চ) ভাইরাস বা ম্যালওয়্যার থেকে সুরক্ষায় ই-মেইলে আগত .exe,.bat, .vbs, .scr এ ধরনের ফাইল খোলা থেকে বিরত থাকা;
ছ) সন্দেহজনক ই-মেইল বা সংযুক্তি না খোলা;
জ) ই-মেইল থেকে নিয়মিত অপ্রয়োজনীয় তথ্যাদি অপসারণ করা; এবং
ঝ) খুব বেশী জরুরি না হলে অন্যের কম্পিউটার থেকে ই-মেইল, সোশ্যাল মিডিয়া প্লাটফর্ম ইত্যাদিতে লগইন করা থেকে বিরত থাকা।

৩.৬.৭ 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 সিসিটিভির মাধ্যমে নজরদারির ব্যবস্থা রাখা;
ঙ) ভেন্ডরদের সার্ভার কক্ষে প্রবেশের তথ্য রেজিস্টারে লিপিবদ্ধ রাখা;
চ) ফিঙ্গারপ্রিন্টসহ অন্যান্য বায়োমেট্রিক সিকিউরিটি সিস্টেমের ব্যবস্থা রাখা;
ছ) স্বয়ংক্রিয় অগ্নিনির্বাপন সিস্টেমের ব্যবস্থা রাখা; এবং
জ) Smoke/Petrol Sensor সিস্টেমের ব্যবস্থা রাখা।

৩.৬.৮ 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 এবং
ঘ) মন্ত্রিপরিষদ বিভাগ কর্তৃক জারিকৃত সরকারি প্রতিষ্ঠানে সামাজিক যোগাযোগ মাধ্যম ব্যবহার সংক্রান্ত নির্দেশিকা, ২০১৬ যথাযথভাবে অনুসরণ করা।

৩.৭ তথ্য নিরাপত্তার আইনগত বিষয়সমূহ:

তথ্য নিরাপত্তায় আইনগত ও প্রায়োগিক বিষয়সমূহ সম্পর্কে সচেতন থাকতে হবে। আইন বা নিয়মের বাধ্যবাধকতার ক্ষেত্রে যে কোন ব্যত্যয় এড়াতে এবং অন্যান্য পলিসির সঙ্গে বিরোধ এড়াতে আইন ও প্রায়োগিক সংক্রান্ত বাহ্যিক ও অভ্যন্তরীণ উভয় বিষয় বিবেচনা করা গুরুত্বপূর্ণ। এ ক্ষেত্রে নিম্নোক্ত আইন, পলিসি, গাইডলাইন প্রভৃতি বিষয়ের প্রতি লক্ষ্য রাখা যেতে পারে:

(১) তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০০৯);
(২) তথ্য ও যোগাযোগ প্রযুক্তি পলিসি, ২০১৫;
(৩) তথ্য অধিকার আইন, ২০০৯;
(৪) দি পেটেন্ট অ্যান্ড ডিজাইন অ্যাক্ট, ১৯১১;
(৫) কপিরাইট অ্যাক্ট, ২০০০ (২০০৫-এ সংশোধিত);
(৬) ক্রিপটোগ্রাফিক নিয়ন্ত্রণের জন্য **PKI** সম্পর্কিত বিধি/২০১০;
(৭) জাতীয় আর্কাইভ আইন, ১৯৮৩;
(৮) সাইবার নিরাপত্তা সম্পর্কিত বিভিন্ন আইন/গাইডলাইন/পলিসি; এবং
(৯) জাতিসংঘ কনভেনশন/ইন্টারনেট বা সাইবার নিরাপত্তা সম্পর্কিত আইন ইত্যাদি।

৩.৮ ঝুঁকি ব্যবস্থাপনা:

ঝুঁকি ব্যবস্থাপনার উদ্দেশ্য হল হুমকি ও অরক্ষিত অবস্থা চিহ্নিত করে তথ্যসম্পদের সংরক্ষণ নিশ্চিত করার জন্য প্রয়োজনীয় কার্যক্রম গ্রহণ করা। ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া অভ্যন্তরীণ ও বাহ্যিক ব্যবস্থার মাধ্যমে সম্পন্ন করা যেতে পারে। ঝুঁকি ব্যবস্থাপনা কার্যক্রম সুষ্ঠুভাবে সম্পাদনের জন্য নিম্নোক্ত বিষয়সমূহ বিবেচনায় রাখতে হবে:

ক. নেটওয়ার্ক এবং সফট্ওয়্যার ডিজাইন ও উন্নয়ন;
খ. নিয়মিত টেকনোলজি প্লাটফর্ম পরিবর্তন;
গ. ভৌত নিরাপত্তা নিশ্চিতকরণ ও প্রবেশাধিকার নিয়ন্ত্রণ;
ঘ. বাহ্যিক এবং অভ্যন্তরীণ ব্যবস্থায় সুরক্ষা বিধান;
ঙ. তথ্য যথাযথভাবে সংরক্ষণ ও ব্যাকআপ কৌশল অবলম্বন;
চ. অপ্রয়োজনীয় তথ্যসম্পদ অপসারণ;
ছ. কম্পিউটার ব্যবহারকারীদের দক্ষতা উন্নয়ন;
জ. আকস্মিক ঘটনা ব্যবস্থাপনার ইতিহাস পর্যালোচনা; এবং
ঝ. সিস্টেম অডিটকরণ (অভ্যন্তরীণ ও বাহ্যিক) ইত্যাদি।

৩.৮.১ ঝুঁকির ক্ষেত্র শনাক্তকরণ:

ঝুঁকির ক্ষেত্র শনাক্তকরণ ঝুঁকি ব্যবস্থাপনার ক্ষেত্রে অত্যন্ত গুরুত্বপূর্ণ। এ ক্ষেত্র শনাক্ত করার উদ্দেশ্য হল বিভিন্ন প্রতিষ্ঠানের তথ্যসম্পদ সুরক্ষার ক্ষেত্রে যে সকল প্রতিবন্ধকতা দেখা যায় তা যথাযথ বিশ্লেষণ ও তার উপযুক্ত প্রতিকারের ক্ষেত্র চিহ্নিত করে প্রয়োজনীয় ব্যবস্থা গ্রহণ। ঝুঁকি শনাক্তকরণ প্রক্রিয়া বাহ্যিক ও অভ্যন্তরীণ হতে পারে। এ ক্ষেত্রে যে সকল বৈশিষ্ট্যে তথ্যের ঝুঁকি নির্ধারিত হবে সে সকল বৈশিষ্ট্যসমূহ সুস্পষ্টভাবে ব্যাখ্যা করা প্রয়োজন।

৩.৮.২ ঝুঁকি চিহ্নিত করা:

কোন প্রতিষ্ঠানের ঝুঁকির ক্ষেত্রসমূহ শনাক্তকরণের পরবর্তী ধাপ হল এ সকল ক্ষেত্রের মধ্যে প্রতিষ্ঠানের কোথায়, কখন, কীভাবে কোন প্রকৃতির আকস্মিক ঘটনা ঘটতে পারে তা যথাযথভাবে চিহ্নিত করা। এ প্রক্রিয়ায় কোন প্রতিষ্ঠানের তথ্যসম্পদের ঝুঁকিসমূহ এমনভাবে চিহ্নিত করা দরকার যাতে তথ্যসম্পদে যে সকল আকস্মিক ঘটনা ঘটার সম্ভাবনা রয়েছে বা ভবিষ্যতে ঘটতে পারে তার প্রতিটি বিষয় পুঙ্খানুপুঙ্খভাবে শনাক্ত করে সে বিষয়সমূহে গুরুত্ব প্রদান করা প্রয়োজন।

৩.৮.৩ ঝুঁকি বিশ্লেষণ:

ঝুঁকি বিশ্লেষণের গুরুত্ব তথ্যসম্পদের ঝুঁকি ব্যবস্থাপনায় অপরিসীম। ঝুঁকি বিশ্লেষণের জন্য বিদ্যমান এবং সম্ভাব্য সকল ঝুঁকির পরিমাপ করা প্রয়োজন। ঝুঁকি পরিমাপের পর প্রতিষ্ঠানকে তার বিদ্যমান নিয়ন্ত্রণ ব্যবস্থার আলোকে ঝুঁকিসমূহ পর্যালোচনা ও মূল্যায়ন করতে হবে। অতঃপর সম্ভাব্য আকস্মিক ঘটনার ফলে তথ্য ব্যবস্থার সম্ভাব্য পরিণতি নির্ধারণ করতে হবে যা ঝুঁকির মাত্রা নির্ণয় এবং ঝুঁকি নিয়ন্ত্রণ করতে সহায়তা করবে। এ বিশ্লেষণের সময় সম্ভাব্য সকল ফলাফল এবং কীভাবে এ সকল ঘটনা ঘটতে পারে তা বিবেচনায় নেওয়া প্রয়োজন।

৩.৮.৪ ঝুঁকি মূল্যায়নঃ

ঝুঁকি প্রশমন করার জন্য ঝুঁকি মূল্যায়ন অত্যন্ত গুরুত্বপূর্ণ। ঝুঁকি বিশ্লেষণের ফলাফলের ওপর ভিত্তি করে প্রতিষ্ঠান তার ঝুঁকিসমূহকে কিভাবে প্রশমন করবে সে বিষয়ে সিদ্ধান্ত গ্রহণ করার জন্য ঝুঁকির ফলাফল ও ঝুঁকির মাত্রা বিবেচনা করে একটি সার্বিক কর্মপরিকল্পনা প্রণয়ন করবে। যথাযথভাবে ঝুঁকি মূল্যায়ন প্রতিষ্ঠানের গুরুত্বপূর্ণ ঝুঁকিসমূহ অগ্রাধিকার ভিত্তিতে প্রশমনের কৌশল নির্ধারণ করার ক্ষেত্রে সহায়তা করে।

৩.৮.৫ ঝুঁকি অপসারণঃ

ঝুঁকি মূল্যায়ন হতে প্রাপ্ত ফলাফল অনুযায়ী প্রতিষ্ঠানকে তার কার্যকর ঝুঁকি নিরসনের পদ্ধতি প্রণয়ন করতে হবে। এ ক্ষেত্রে জনবল এবং তথ্যপ্রযুক্তির সর্বোচ্চ দক্ষতা কাজে লাগিয়ে স্বল্প সময়ে সর্বনিম্ন ব্যয়ে বাস্তবায়নযোগ্য বিষয়সমূহ বিবেচনা করতে হবে। প্রয়োজনে পরামর্শক প্রতিষ্ঠানের সহযোগিতা নিয়েও ঝুঁকি নিরসন করা যেতে পারে। ঝুঁকি অপসারণ বা নিয়ন্ত্রণ বিভিন্ন পর্যায়ে হতে পারে। যেমনঃ

ক. ঘটনা ঘটার পূর্বে, প্রতিরোধমূলক ব্যবস্থার মাধ্যমে ঝুঁকি অপসারণ;

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

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

৩.৯ তথ্য নিরাপত্তা সম্পর্কিত প্রশিক্ষণঃ

প্রতিষ্ঠানের জন্য দক্ষ মানবসম্পদের গুরুত্ব অপরিসীম। যথাযথ প্রশিক্ষণের মাধ্যমেই প্রতিষ্ঠানে দক্ষ মানবসম্পদ গড়ে তোলা সম্ভব। বর্তমানে তথ্য ও যোগাযোগ প্রযুক্তির ক্ষেত্রে প্রতিনিয়ত নতুন নতুন প্রযুক্তির আবির্ভাব ঘটছে। এ সকল প্রযুক্তিকে যথাযথভাবে কাজে লাগানোর জন্য প্রশিক্ষণ কার্যক্রম আরও বেশি জোরদার করা প্রয়োজন। উপযুক্ত প্রশিক্ষণ প্রদানের মাধ্যমেই একটি প্রতিষ্ঠানের তথ্য সুরক্ষা ও তথ্যের যথাযথ ব্যবহার নিশ্চিত করা সম্ভব হয়। লক্ষ্য করা যাচ্ছে যে, তথ্যপ্রযুক্তিতে অত্যন্ত দক্ষ ও অভিজ্ঞ ব্যক্তিগণ বর্তমানে সারা বিশ্বে হ্যাকিং কার্যক্রম পরিচালনা করছে এবং হ্যাকিং-এর ক্ষেত্রে তারা প্রতিনিয়ত নতুন নতুন কৌশল অবলম্বন করছে। প্রতিষ্ঠানের তথ্যসম্পদকে এ সকল অনৈতিক কার্যক্রম হতে যথাযথভাবে প্রতিরোধ করার লক্ষ্যে প্রয়োজন তথ্য নিরাপত্তা বিষয়ক নিবিড় প্রশিক্ষণ। এ ক্ষেত্রে নিম্নোক্ত কার্যক্রম গ্রহণ করা যেতে পারেঃ

ক) তথ্যের নিরাপত্তা বিষয়ে সচেতনতা বৃদ্ধির লক্ষ্যে প্রতিষ্ঠানের সংশ্লিষ্ট কর্মকর্তা-কর্মচারীদের জন্য নিয়মিত প্রশিক্ষণ আয়োজন করা;

খ) তথ্য নিরাপত্তার বিষয়ে প্রতিষ্ঠানে নিয়মিত সেমিনার, ওয়ার্কশপ ইত্যাদি আয়োজন করা;

গ) তথ্য নিরাপত্তা বিষয়ে প্রাতিষ্ঠানিক প্রশিক্ষণ কর্মপরিকল্পনা ও কর্মসূচি গ্রহণ এবং তা বাস্তবায়ন করা;

ঘ) তথ্য নিরাপত্তা বিষয়ে প্রশিক্ষণের জন্য পর্যাপ্ত বাজেট বরাদ্দ রাখা; এবং

ঙ) তথ্য নিরাপত্তার সঙ্গে সংশ্লিষ্টদের জন্য দেশে-বিদেশ উচ্চতর প্রশিক্ষণের ব্যবস্থা রাখা।

৩.১০ তথ্য ব্যবস্থাপনা নিরীক্ষা ও প্রত্যয়নঃ

(১) কোন প্রতিষ্ঠানের তথ্য ব্যবস্থাপনা পরিচালনা পদ্ধতির যে কোন ধরনের বিপর্যয় ন্যূনতম পর্যায়ে রাখাসহ এ কর্মতৎপরতার উন্নয়নে তথ্য ব্যবস্থাপনা নিরীক্ষা অত্যন্ত গুরুত্বপূর্ণ। যে সকল প্রতিষ্ঠান গুরুত্বপূর্ণ তথ্য ব্যবস্থাপনা অবকাঠামো পরিচালনা করে থাকে তাদের অবশ্যই সময়ে সময়ে তথ্য নিরীক্ষা করা প্রয়োজন। এ ক্ষেত্রে তথ্য ব্যবস্থাপনায় বিশেষায়িত নিরীক্ষা সংস্থার মাধ্যমে নিরীক্ষা পরিচালনা করার পাশাপাশি প্রতিষ্ঠানের অভ্যন্তরীণ সংশ্লিষ্ট বিষয়ে বিশেষজ্ঞ জনবলের মাধ্যমেও নিয়মিত নিরীক্ষা কার্যক্রম পরিচালনা করা যেতে পারে।

(২) প্রত্যয়ন হল কোন তৃতীয় পক্ষ কর্তৃক কোন প্রতিষ্ঠানের তথ্য ব্যবস্থাপনা অবকাঠামো এবং তথ্য নিরাপত্তা ব্যবস্থাপনা পদ্ধতি যাচাইয়ের ভিত্তিতে এক ধরনের বাহ্যিক মূল্যায়ন। মূল্যায়নের নির্ণায়কসমূহ সর্বদাই মানদণ্ড কর্তৃপক্ষ কর্তৃক নিয়ন্ত্রিত হয়ে থাকে। মূলত এ প্রত্যয়নের মাধ্যমে কোন প্রতিষ্ঠানের বিষয়ে উক্ত প্রতিষ্ঠানের অংশীজনেরা তথ্য নিরাপত্তা নিশ্চয়তা উপলব্ধি করতে পারেন। কোন প্রতিষ্ঠান ISO/IEC ২৭০০১ অনুযায়ী প্রত্যয়ন প্রত্যাশা করার পূর্বেই মূল্যায়নের নির্ণায়কসমূহ জেনে নেওয়া প্রয়োজন। মান বিষয়ক প্রত্যয়ন প্রতিষ্ঠানসমূহের কর্মপরিবেশ ও কর্মক্ষমতা উন্নয়নে সহায়তা করে।

৩.১১ আকস্মিক ঘটনা ব্যবস্থাপনাঃ

(১) তথ্য নিরাপত্তায় আকস্মিক ঘটনা হল এক বা একাধিক অনাকাঙ্ক্ষিত বা অপ্রত্যাশিত তথ্য নিরাপত্তা বিষয়ক ঘটনা, যার কারণে প্রতিষ্ঠানে স্বাভাবিক কর্মকাণ্ড পরিচালনায় বিঘ্ন ঘটে। তথ্য নিরাপত্তার ক্ষেত্রে কোন আকস্মিক ঘটনা ঘটার পূর্বেই এ বিষয়ে পরিকল্পনা গ্রহণ করা খুবই গুরুত্বপূর্ণ। যদিও কখন কি ধরনের অনাকাঙ্ক্ষিত ঘটনা ঘটবে তা পূর্বেই সঠিকভাবে জানা সম্ভব নয়। তবুও তথ্য নিরাপত্তায় যে কোন ধরনের দূর্ঘটনা যে কোন সময় ঘটতে পারে এ বিবেচনায় প্রতিষ্ঠানের যথাযথ সতর্কতা অবলম্বন করা প্রয়োজন। এ জন্য যে কোন প্রতিষ্ঠানে আকস্মিক ঘটনা মোকাবিলায় শক্তিশালী ও কার্যকর নিয়ন্ত্রণ ব্যবস্থা প্রতিষ্ঠা করা খুবই জরুরি।

(২) আকস্মিক ঘটনা প্রাকৃতিক অথবা মনুষ্য-সৃষ্ট হতে পারে। উভয়ক্ষেত্রে ঘটনা মোকাবিলায় সুচারূভাবে কার্যকর পদক্ষেপ গ্রহণ করতে হবে। যে কোন ধরনের প্রাকৃতিক দুর্যোগের সময় যেমনঃ বন্যা, অগ্নিকাণ্ড, ভূমিকম্প প্রভৃতি আকস্মিক ঘটনায় দাপ্তরিক কার্যক্রমের ধারাবাহিকতা রক্ষার্থে স্বল্প সময়ের মধ্যে তথ্য ব্যবস্থা পুনরুদ্ধারের কার্যক্রম শুরু করা প্রয়োজন।

(৩) তথ্য নিরাপত্তায় মনুষ্য-সৃষ্ট আকস্মিক ঘটনার ক্ষেত্রে যথাশীঘ্র সম্ভব ঊর্ধ্বতন কর্তৃপক্ষকে অবহিত করা প্রয়োজন। এ বিষয়ে তথ্য নিরাপত্তা বিষয়ক বিশেষজ্ঞ দলকে (অভ্যন্তরীণ/বাহিরের) ঘটনা ঘটার পরপরই তদন্তপূর্বক যথাযথ রিপোর্ট প্রদান করার জন্য দায়িত্ব প্রদান করা যেতে পারে। কোন আকস্মিক ঘটনার তদন্তের পর সংশ্লিষ্ট রেকর্ডসমূহ সংরক্ষণ করে রাখতে হবে। অধিকন্তু, এ ধরনের মূল্যায়ন-রিপোর্ট প্রয়োজনীয়তার নিরিখে যথাযথ কার্যক্রম গ্রহণের নিমিত্ত ঊর্ধ্বতন কর্তৃপক্ষকে অবহিত করতে হবে।

(৪) আকস্মিক ঘটনা মোকাবিলায় মন্ত্রিপরিষদ বিভাগে একটি জরুরি সাড়া প্রদানকারী টিম গঠন করা প্রয়োজন। অনেক ক্ষেত্রে লক্ষ্য করা যায় এ ধরনের পরিস্থিতি শুধুমাত্র প্রতিষ্ঠানের নিজস্ব জনবলের দ্বারা মোকাবিলা করা সম্ভব হয় না। এ কারণে জুরুরি সাড়া প্রদানকারী টিম গঠনের

ক্ষেত্রে নিজস্ব জনবলের পাশাপাশি বাইরের বিশেষায়িত প্রতিষ্ঠানের সদস্যগণকেও অন্তর্ভুক্ত করা যেতে পারে। এ টিমের সদস্যগণ আকস্মিক ঘটনা মোকাবেলায় কীভাবে অবদান রাখবে সে বিষয়ে কর্মপরিকল্পণা প্রণয়ন করতে হবে।

৩.১২ তথ্য নিরাপত্তা প্রতিষ্ঠায় অনুসৃত মানদণ্ড:

এ তথ্য নিরাপত্তা নির্দেশিকা বাস্তবায়নের ধাপসমূহ নির্দেশিকার সফল বাস্তবায়নের ক্ষেত্রে অনুসৃত কোন মানদন্ডের ব্যাখ্যা প্রদান করে না। নির্দেশিকা অনুসরণের সময়ই মানদণ্ড ও নির্দেশনা কাজে আসে। তথ্যসম্পদ সুরক্ষার পলিসি ডকুমেন্ট প্রণয়নে প্রতিটি পর্যায়ে আবশ্যিকভাবে প্রতিষ্ঠান কর্তৃক মানদন্ড নির্ধারণের কিছু নির্দেশনা থাকা প্রয়োজন। পলিসি ডকুমেন্টে প্রয়োজনীয়তার নিরিখে এ সকল নির্দেশনা ও মানদণ্ড অন্তর্ভুক্ত হতে পারে।

৩.১৩ বাস্তবায়ন, পরিবীক্ষণ ও মূল্যায়ন:

ক.বাস্তবায়ন:

তথ্য নিরাপত্তায় এ নির্দেশিকার বর্ণিত বিষয়সমূহ বাস্তবায়নে মন্ত্রিপরিষদ বিভাগ কর্তৃক যথাযথ কার্যকর পদক্ষেপ গ্রহণ করা প্রয়োজন। এ নির্দেশিকাটি অনুসরণের মাধ্যমে তথ্য নিরাপত্তা বিষয়ে এ বিভাগের জনবলের দক্ষতা বৃদ্ধির লক্ষ্যে প্রশিক্ষণ কর্মসূচি গ্রহণ ও বাস্তবায়ন করা যেতে পারে। নিয়মিত সভা, সেমিনার, ওয়ার্কশপ ইত্যাদি আয়োজন করা হলে নতুন নতুন যে সকল ঝুঁকির সম্ভাবনা দেখা দিবে তা নিরসনে কার্যকর পদক্ষেপ গ্রহণ করা সম্ভব হবে। এ সকল কার্যক্রম চালু রাখার পাশাপাশি তথ্য নিরাপত্তা বিষয়ে সচেতনতা বৃদ্ধিসহ অন্যান্য কার্যক্রম অব্যাহত রাখা প্রয়োজন।

খ.পরিবীক্ষণ ও মূল্যায়ন:

তথ্য নিরাপত্তা ব্যবস্থাপনায় পরিবীক্ষণ ও মূল্যায়ন কৌশলের গুরুত্ব অপরিসীম। সময়ের ব্যবধানে তথ্যের নতুন নতুন হুমকি/ঝুঁকির আবির্ভাব হয় বলে তথ্য ব্যবস্থাপনার ক্ষেত্রে নিয়মিত পরিবীক্ষণ ও মূল্যায়ন করে নতুন নতুন কার্যক্রম গ্রহণ করার প্রয়োজন হয়। অনেক ক্ষেত্রে তথ্য প্রযুক্তির সঙ্গে সংশ্লিষ্ট কর্মকর্তা-কর্মচারীদের বদলিজনিত কারনে নতুন সমস্যার সৃষ্টি হতে পারে সে বিষয়টিও পরিবীক্ষণ ও মূল্যায়নের আওতায় আনা প্রয়োজন। নবসৃষ্ট কোন বিষয় যদি তথ্য নিরাপত্তার জন্য হুমকি হয় তবে সে ক্ষেত্রেও নিরাপত্তার নিয়ন্ত্রণসমূহে পরিবর্তন আনার বিষয়টি বিবেচনায় রাখতে হবে। সার্ভার, নেটওয়ার্ক, হার্ডওয়্যার, সফট্ওয়্যার, এন্টিভাইরাস ব্যবস্থাপনা, ইন্টারনেট ব্যান্ডউইথ ব্যবস্থাপনা, পাসওয়ার্ড ব্যবস্থাপনা ইত্যাদি সার্বক্ষণিক পরিবীক্ষণের আওতায় থাকা আবশ্যক। একই সঙ্গে নিয়মিত পরিবীক্ষণের ফলাফলের ভিত্তিতে মূল্যায়ন করে তথ্য নিরাপত্তায় প্রয়োজনীয় কার্যক্রম গ্রহণ করা প্রয়োজন।

পরিশিষ্ট: তথ্যসূত্র

১. তথ্য নিরাপত্তা পলিসি গাইডলাইন (বাংলা ভার্সন), তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ;

২. Guideline on ICT security for Banks and Non-Bank Financial Institutions, May 2015;

৩. ISO/IEC 27000:2009, Information security management systems Overview and vocabulary;

৪ ISO/IEC 27001:2005, Information security management systems requirements;

৫. ISO/IEC 27002:2005, Code of practice for information security management;

৬. ISO/IEC 27003, Information security management system implementation guidance;

৭. ISO/IEC 27004, Information security managemen - Measurement;

৮. ISO/IEC 27005:2008, Information security risk management;

৯. ISO/IEC 27007, Guidelines for information security management systems auditing;

১০. ISO/IEC 27011, Information security management guidelines or telecommunications organizations based on ISO/IEC 27002;

১১. ISO 31000:2009 Risk management - Principles and guidelines.