

রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ



গেজেট

অতিরিক্ত সংখ্যা
কর্তৃপক্ষ কর্তৃক প্রকাশিত

রবিবার, এপ্রিল ৬, ২০১৪

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ
(আইসিটি-১ শাখা)

প্রজ্ঞাপন

তারিখ, ২৪ মার্চ ২০১৪ খ্রিঃ

নং ৫৬.০০.০০০০.০২৫.২২.০০২.১৪-৩৬—সরকার তথ্য নিরাপত্তা নিশ্চিত করার লক্ষে “তথ্য নিরাপত্তা পলিসি গাইডলাইন” এর বাংলা ও ইংরেজী ভার্সন অনুমোদন করেছে। ইহা সর্বসাধারণের জ্ঞাতার্থে প্রকাশ করা হলো।

রাষ্ট্রপতির আদেশক্রমে

আর. এইচ. এম. আলাওল কবির
সহকারী সচিব।

(১২৫১৯)

মূল্য : টাকা ৪৮.০০

১। প্রস্তাবনা

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার “রূপকল্প ২০২১: ডিজিটাল বাংলাদেশ” বিনির্মাণে বন্ধপরিকর। এই লক্ষ্য অর্জন করিতে হইলে সকল সরকারি সংস্থাকে ই-গভর্নেন্স কাঠামোর আওতায় আনিতে হইবে। সরকারের বিভিন্ন মন্ত্রণালয়/বিভাগ, অধিদপ্তর/সংস্থা ও তাহাদের অধীন প্রতিষ্ঠানসমূহ ই-গভর্নেন্স বাস্তবায়নের কাজ করিতেছে। সরকারি কর্মপ্রক্রিয়ার উন্নয়ন ও সহজীকরণ এবং সরকারের সক্ষমতা বৃদ্ধি করাই ইহার উদ্দেশ্য। ইহা করিতে হইলে তথ্য ডিজিটালকরণ করিতে হইবে এবং সেই সকল ডিজিটালকৃত তথ্য এইরূপভাবে প্রক্রিয়া ও সংরক্ষণ করিতে হইবে যাহাতে তথ্যসমূহ হারাইয়া না যায় কিংবা ইহার অপব্যবহার না হয়। সাম্প্রতিককালে বাংলাদেশ তথ্য সুরক্ষা বিষয়ক কার্যপ্রণালির অভাব, দুর্বল ও অব্যবস্থাপনাজনিত নিরাপত্তা নিয়ন্ত্রণ ব্যবস্থা, স্বল্পদক্ষ কর্মচারী কর্তৃক ব্যবস্থাপনা পরিচালিত হওয়া এবং বিশেষায়িত জ্ঞান ও দক্ষতার অভাবসহ নানা কারণে একাধিকবার ওয়েব ডিফেইসমেন্ট, তথ্য বিপর্যয়, তথ্য চুরি, ডিসট্রিবিউটেড ডিনাইয়াল অব সার্ভিস ইত্যাদির মাধ্যমে সাইবার আক্রমণের শিকার হইয়াছে। এইসব আক্রমণের বিরুদ্ধে ডিজিটালকৃত সরকারি তথ্য সম্পদ সুরক্ষার লক্ষ্যে পর্যাপ্ত প্রতিরোধক, নিরোধক, অনুসন্ধানী ও প্রশাসনিক নিরাপত্তামূলক ব্যবস্থা নাই। তাই ডিজিটালকৃত সরকারি তথ্য সম্পদে অননুমোদিত অনুপ্রবেশ রোধ করিতে সঠিক নিরাপত্তা পলিসি ও বাস্তবায়ন কৌশল প্রণয়ন অপরিহার্য। এই দলিলটি সেই সকল সংস্থার জন্য প্রণীত হইয়াছে যাহারা তাহাদের ডিজিটালকৃত তথ্য সাইবার স্পেসে সুরক্ষা করিবার উদ্দেশ্যে নিজস্ব তথ্য নিরাপত্তা কৌশল প্রণয়ন করিতে চাহে। দলিলটি সেই সকল সংস্থার জন্য একটি সহায়ক নির্দেশনাপত্র হিসাবে কাজ করিবে।

২। ভূমিকা

(১) তথ্য একটি সংস্থার সর্বাধিক মূল্যবান সম্পদ। প্রবেশাধিকারের বিবেচনায় তথ্যের বিভিন্ন প্রকারভেদ রহিয়াছে। কিছু তথ্য উন্মুক্ত আবার কিছু তথ্য গোপনীয়। গোপনীয়তার মাত্রার ভিত্তিতে তথ্যে প্রবেশাধিকারেরও বেশ কয়েকটি পর্যায় রহিয়াছে; যেমন কিছু তথ্য কোনো রকম প্রমাণীকরণ ছাড়াই সর্বসাধারণের ব্যবহারের জন্য উন্মুক্ত; কিছু তথ্য একক-উৎস কর্তৃক প্রমাণীকরণ সাপেক্ষ; কিছু তথ্যের জন্য প্রয়োজন একাধিক প্রমাণীকরণ; আবার কিছু তথ্য প্রতিষ্ঠানের নিজস্ব; কিছু তথ্য অতি গোপনীয় যাহা প্রতিষ্ঠানের নির্দিষ্ট কিছু লোক ব্যবহার করিয়া থাকে। সুতরাং একটি সংস্থার তথ্য ও তাহাতে প্রবেশাধিকার বিষয়ে স্বচ্ছ ধারণা থাকা অত্যাবশ্যক। তথ্য নিরাপত্তা পলিসি প্রণয়নের পূর্বে সংস্থার তথ্যসমূহ সঠিকভাবে যাচাইয়ের মাধ্যমে শ্রেণিবিন্যাস করা প্রয়োজন।

(২) সকলের জন্য তথ্যের উন্মুক্ত ক্ষেত্র হইল ইন্টারনেট। ইন্টারনেট ও অন্যান্য প্রযুক্তি, যেমন-হস্তে ধারণযোগ্য (Hand-held) যন্ত্র, মোবাইল প্রযুক্তি, ট্যাবলেট পিসি, বেতার প্রযুক্তি তথ্যকে সহজলভ্য ও সাশ্রয়ী করিয়াছে। অন্যদিকে দেশে বিশৃঙ্খলা সৃষ্টির হাতিয়ার হিসেবে তথ্য ব্যবহৃত হইতে পারে। সুতরাং ইন্টারনেটে প্রদত্ত তথ্য সম্পর্কে সংস্থাকে দায়িত্বশীল ভূমিকা পালন করিতে হইবে। আবার ইন্টারনেটে প্রদত্ত তথ্য ছাড়াও সংস্থাকে বিভিন্ন মাধ্যমে সঞ্চালিত ও সঞ্চিত তথ্য সম্পর্কেও সতর্ক থাকিতে হইবে, যেমন-ইন্ট্রানেট বা ল্যান (LAN)-এ সঞ্চালিত তথ্য বা ক্লাউড (Cloud) এ কিংবা অভ্যন্তরীণ তথ্যভান্ডার (Database) বা কম্পিউটারে (PC) সঞ্চিত তথ্য।

(৩) এই নির্দেশনাপত্রে যাহা রহিয়াছে তাহা হইল:

- ক. বিভিন্ন পরিভাষার (Terminology) সংক্ষিপ্ত বিবরণ (Illustration) যাহা তথ্য নিরাপত্তা পলিসি প্রণয়নের জন্য জানা প্রয়োজন,
- খ. এই নির্দেশনাপত্রের উদ্দেশ্য,
- গ. এই নির্দেশনাপত্রের পরিধি (Scope),

- ঘ. তথ্যের শ্রেণিকরণ এবং তথ্যের বিভিন্ন অবস্থা,
- ঙ. তথ্যের সত্ত্বাধিকারী ও তথ্য রক্ষকের ভূমিকা ও দায়িত্ব,
- চ. তথ্য নিরাপত্তা কৌশল,
- ছ. সম্ভাব্য ঝুঁকি, বিপদের আশঙ্কা ও দুর্বল স্থান চিহ্নিতকরণ,
- জ. ঝুঁকি, বিপদের আশঙ্কা ও দুর্বলস্থান পরিমাপকরণ,
- ঝ. তথ্য সংরক্ষণে নিরাপত্তা নিয়ন্ত্রণ সংযোগ করিবার প্রণালি,
- ঞ. তথ্য নিরাপত্তার আইনগত বিষয়সমূহ,
- ট. তথ্য নিরাপত্তাবিষয়ক ব্যবস্থাপনা পদ্ধতি (ISMS) প্রতিষ্ঠায় অনুসৃত মানদণ্ড,
- ঠ. তথ্য নিরাপত্তার জন্য অডিট করানোর গুরুত্ব,
- ড. পরিবীক্ষণ ও উন্নয়ন,
- ঢ. সংস্থা হিসাবে প্রত্যয়ন,
- ণ. আকস্মিক ঘটনা নিয়ন্ত্রণ ও বিপর্যয় হইতে পরিত্রাণের উপায়,
- ত. পরিপূরণ ও পুনর্বহাল কৌশল,
- থ. কার্যক্রমে ধারাবাহিক পরিকল্পনা,
- দ. তথ্য নিরাপত্তা পলিসির নমুনা।

৩। পলিসি গাইডলাইন অনুসরণ ও বলবৎকরণ

(১) বাংলাদেশ সরকারের পক্ষে তথ্য ও যোগাযোগ প্রযুক্তি মন্ত্রণালয় এই নির্দেশনাপত্রটির সত্ত্বাধিকারী হইবে। এই মন্ত্রণালয় নির্দেশনাপত্রটির বাস্তবায়ন পরিবীক্ষণ বা তদারিক করিবে। বাংলাদেশ কম্পিউটার কাউন্সিল, কন্ট্রোলার অফ সার্টিফাইং অথরিটি (CCA) ও বাংলাদেশ টেলিযোগাযোগ নিয়ন্ত্রণ কমিশন যৌথভাবে এই নির্দেশনাপত্রের বাস্তবায়ন সমন্বয় করিবে।

(২) বাংলাদেশ সরকারের সকল সংস্থাকে এই নির্দেশনাপত্র কার্যকর হইবার ছয় মাসের মধ্যে তাহাদের নিজ-নিজ তথ্য নিরাপত্তা পলিসির প্রণয়ন ও উহার বাস্তবায়ন করিতে অনুরোধ করা হইবে। এই দলিল সম্পর্কে কোনো প্রশ্ন থাকিলে তাহা তথ্য ও যোগাযোগ প্রযুক্তি মন্ত্রণালয় অথবা বাংলাদেশ কম্পিউটার কাউন্সিলকে অবহিত করা যাইবে। যদি কোনো সংস্থার তথ্য নিরাপত্তা পলিসি প্রণয়নে সহায়তা প্রয়োজন হয়, তাহা হইলে সেই বিষয়ে বাংলাদেশ কম্পিউটার কাউন্সিলকে অনুরোধ করা যাইবে।

৪। সংজ্ঞা

(১) “সংস্থা” অর্থ বাংলাদেশ সরকারের মন্ত্রণালয়/বিভাগ, অধিদপ্তর/পরিদপ্তর, মন্ত্রণালয়ের আওতাধীন সংস্থা, বিধিবদ্ধ সংস্থা ও উহাদের অধীন প্রতিষ্ঠানসমূহ।

(২) “সম্পদ” অর্থ সংস্থায় নিকট মূল্য রহিয়াছে এমন সকল কিছু।

(৩) “আক্রমণ” অর্থ কোনো সম্পদ ধ্বংস, উন্মুক্ত, পরিবর্তন, অকেজো, চুরি করিবার অথবা উহাতে অননুমোদিত উপায়ে প্রবেশ বা উহা অননুমোদিতভাবে ব্যবহার করিবার প্রচেষ্টা।

(৪) “প্রমাণীকরণ” অর্থ একটি স্বতন্ত্র সত্ত্বার (entity) বৈশিষ্ট্য সঠিক হইবার বিষয়ে নিশ্চয়তা প্রদানের বিধান প্রমাণ্যতা: একটি স্বতন্ত্র সত্ত্বা যেইরূপ হইবার দাবি করে সেইরূপ হইবার বৈশিষ্ট্য।

- (৫) “যথার্থতা” অর্থ একটি স্বতন্ত্র সত্ত্বা (entity) যেইরূপ হইবার দাবি করে সেইরূপ হইবার বৈশিষ্ট্য।
- (৬) “লভ্যতা” অর্থ কোনো নির্ধারিত সময়-সীমার মধ্যে একজন ব্যবহারকারীর নিকট প্রাপ্তিযোগ্য তথ্য ব্যবস্থা (Information Systems) যাহা অনুমোদিত সত্ত্বার চাহিদা অনুযায়ী প্রবেশযোগ্য ও ব্যবহারযোগ্য।
- (৭) “কার্যক্রমের ধারাবাহিকতা” অর্থ চলমান কার্যক্রম নিশ্চিতকরণের প্রক্রিয়া।
- (৮) “গোপনীয়” অর্থ অননুমোদিত কোনো ব্যক্তি, স্বতন্ত্র সত্ত্বা (entity), কোনো ব্যবস্থা (System) বা প্রক্রিয়া তথ্য প্রাপ্ত হইবে না কিংবা উহাদের নিকট তথ্য প্রকাশ করা হইবে না।
- (৯) “প্রত্যয়ন” অর্থ কোন মান নির্ধারণকারী প্রতিষ্ঠান বা প্রতিষ্ঠানের বাহিরের বিশেষজ্ঞ কর্তৃক পর্যালোচনার মাধ্যমে কোন সংস্থাকে তাহাদের তথ্য ব্যবস্থাপনার সাথে সংশ্লিষ্ট অবকাঠামো ও তথ্য নিরাপত্তা ব্যবস্থা বিষয়ক পদ্ধতির মূল্যায়ন।
- (১০) “শ্রেণিকরণকৃত তথ্য” অর্থ নিরাপত্তাবিষয়ক প্রবিধান (The Security Regulations) অনুযায়ী শ্রেণিকরণ করা হইয়াছে এইরূপ তথ্য।
- (১১) “নিয়ন্ত্রণ” অর্থ নিয়ন্ত্রণ বলিতে প্রশাসনিক, কারিগরি, ব্যবস্থাপনাবিষয়ক, কিংবা আইনসংক্রান্ত পলিসি, পদ্ধতি, নির্দেশনা, অনুশীলন বা সাংগঠনিক কাঠামোসহ ঝুঁকি ব্যবস্থাপনাকেই বুঝায়। নিয়ন্ত্রণ নিরাপত্তা বিধান বা বিকল্পব্যবস্থার সমার্থক শব্দ হিসাবেও ব্যবহৃত হয়।
- (১২) “নিয়ন্ত্রণের উদ্দেশ্য” অর্থ নিয়ন্ত্রণসমূহ বাস্তবায়নের ফলস্বরূপ যাহা অর্জিত হইবে তাহার বিবরণ।
- (১৩) “সংশোধনমূলক ব্যবস্থা” অর্থ সনাক্তকৃত কোনো বৈসাদৃশ্য বা অন্য কোনো অনাকাঙ্ক্ষিত অবস্থার কারণ দূরীকরণের ব্যবস্থা।
- (১৪) “আড়িপাতা” অর্থ আড়িপাতা বা তথ্যে অননুমোদিত প্রবেশ এমন এক ধরনের নেটওয়ার্ক আক্রমণ যাহা তথ্য-যোগাযোগ/প্রেরণকালে প্যাকেট দখলের মাধ্যমে করা হইয়া থাকে।
- (১৫) “স্বীয়-স্বার্থে ব্যবহার (Exploit)” অর্থ এমন একটি কৌশল বা কোড যাহার মাধ্যমে কোনো একটি অরক্ষিত অবস্থা ব্যবহার করিয়া আক্রমণকারীর জন্য তথ্য ব্যবস্থায় প্রবেশের সুযোগ সৃষ্টি করা।
- (১৬) “নির্দেশনাপত্র (Guideline)” অর্থ তথ্য প্রক্রিয়াকরণ সুবিধা, অন্য কোনো তথ্য প্রক্রিয়াকরণ ব্যবস্থা, সেবা বা অবকাঠামো কিংবা তাহাদের বাস্তব অবস্থানের পরিপ্রেক্ষিতে পলিসি-তে বিবৃত উদ্দেশ্য অর্জনে কি করিতে হইবে এবং কিভাবে করিতে হইবে তাহার বিবরণ।
- (১৭) “তথ্য ব্যবস্থা” অর্থ তথ্য প্রযুক্তি ব্যবহারের মাধ্যমে ইলেক্ট্রনিক উপায়ে উপাত্ত প্রক্রিয়াকরণের ইলেক্ট্রনিক তথ্য ব্যবস্থা যাহার মধ্যে অন্তর্ভুক্ত রহিয়াছে (যাহা সীমাবদ্ধ থাকিবে না) কম্পিউটার সিস্টেম, সার্ভার, ওয়ার্ক স্টেশন, টার্মিনাল, স্টোরেজ মিডিয়া, কমিউনিকেশন ডিভাইস, নেটওয়ার্ক রিসোর্স ও ইন্টারনেট।
- (১৮) “শুদ্ধতা” অর্থ কেবলমাত্র অনুমোদিত ব্যক্তিদিগকে তথ্য ব্যবস্থার মাধ্যমে স্টোরকৃত বা প্রক্রিয়াকরণকৃত তথ্যে সকল ক্ষেত্রে পরিবর্তন করিতে দেওয়া।
- (১৯) “তথ্য নিরাপত্তা” অর্থ তথ্যের গোপনীয়তা, শুদ্ধতা ও লভ্যতা সংরক্ষণ; ইহা ছাড়া অন্যান্য বৈশিষ্ট্য যেমন প্রামাণ্যতা, জবাবদিহিতা, অনস্বীকৃতি (Non repudiation) ও নির্ভরশীলতাও ইহার অন্তর্ভুক্ত হইতে পারে।

(২০) “তথ্য নিরাপত্তা (আইএস) পলিসি” অর্থ ব্যবস্থাপনাবিষয়ক নির্দেশনাবলির এমন একটি প্রামাণ্য তালিকা যাহা তথ্য-ব্যবস্থাপনায় সঞ্চিত বা প্রক্রিয়াকরণকৃত কোনো অননুমোদিত প্রকাশ, পরিবর্তন বা ক্ষতি হইতে সুরক্ষা করিবার লক্ষ্যে কম্পিউটার ও নেটওয়ার্ক সম্পদের সঠিক ব্যবহার ও ব্যবস্থাপনা সম্পর্কে সবিস্তারে বর্ণনা করে।

(২১) “তথ্য নিরাপত্তা ইভেন্ট” অর্থ তথ্য নিরাপত্তা ইভেন্ট হইল তথ্য ব্যবস্থা, তথ্য সেবা বা নেটওয়ার্ক সম্পর্কিত এমন একটি ঘটনা যাহা তথ্য নিরাপত্তা পলিসির সম্ভাব্য বিচ্যুতি বা সংরক্ষণের ব্যর্থতাকে নির্দেশ করে। ইহা এমন একটি ঘটনাও হইতে পারে যাহা পূর্বে অজানা ছিল এবং যাহা নিরাপত্তার প্রতি হুমকি স্বরূপ।

(২২) “তথ্য নিরাপত্তা ইনসিডেন্ট” অর্থ এক বা একাধিক অনাকাঙ্ক্ষিত বা অপ্রত্যাশিত তথ্য নিরাপত্তা ইভেন্ট যাহা প্রতিষ্ঠানের কার্যক্রম ব্যাহত করিতে পারে ও তথ্য নিরাপত্তার প্রতি হুমকি হিসেবে পরিগণিত হইতে পারে।

(২৩) “পিকেআই (PKI)” অর্থ হার্ডওয়্যার, সফটওয়্যার, পলিসি ও পদ্ধতির সমন্বয়ে গঠিত এমন একটি কাঠামো যাহা তথ্য নিরাপত্তার জন্য (Keys and Certificates) ব্যবস্থাপনায় ব্যবহৃত হয়।

(২৪) “পলিসি” অর্থ ব্যবস্থাপনা কর্তৃপক্ষ কর্তৃক আনুষ্ঠানিকভাবে প্রকাশিত সামগ্রিক উদ্দেশ্য ও নির্দেশনা।

(২৫) “ঝুঁকি বিশ্লেষণ” অর্থ ঝুঁকির উৎস সনাক্তকরণ ও ঝুঁকির পরিমাণ নির্ণয় করা।

(২৬) “ঝুঁকি নির্ধারণ” অর্থ ঝুঁকি বিশ্লেষণ ও মূল্যায়নের সামগ্রিক প্রক্রিয়া।

(২৭) “ঝুঁকি মূল্যায়ন” অর্থ ঝুঁকির মাপকাঠির সহিত পরিমাপকৃত ঝুঁকির তুলনা করিয়া ঝুঁকির মাত্রা নির্ধারণ।

(২৮) “ঝুঁকি ব্যবস্থাপনা” অর্থ ঝুঁকি সম্পর্কে কোনো প্রতিষ্ঠানকে নির্দেশনা প্রদান ও ঝুঁকি নিয়ন্ত্রণ করিবার সমন্বিত কর্মতৎপরতা।

(২৯) “ঝুঁকি নিরসন” অর্থ ঝুঁকি নিয়ন্ত্রণ বা হ্রাস কবির ব্যবস্থা নির্বাচন ও বাস্তবায়নের প্রক্রিয়া।

(৩০) “সামাজিক কৌশল (সোশ্যাল ইঞ্জিনিয়ারিং)” অর্থ ব্যক্তির নিকট হইতে কূটকৌশলের মাধ্যমে তথ্য পাওয়া।

(৩১) “ঠকানো (Spoofing)” অর্থ ছদ্মবেশ ধারণ করিয়া কোন কম্পিউটার সিস্টেমে প্রবেশ করিবার জন্য প্রকৃত আইপি অ্যাড্রেস-এর পরিবর্তে একটি বিশ্বস্ত (Trusted) আইপি অ্যাড্রেস ব্যবহার করা।

(৩২) “তৃতীয় পক্ষ” অর্থ বিবেচ্য বিষয়ের সহিত স্বার্থ সংশ্লিষ্ট ব্যক্তি বা প্রতিষ্ঠান ব্যতীত স্বতন্ত্র ব্যক্তি বা প্রতিষ্ঠান।

৫। উদ্দেশ্য

(১) একটি দেশ বা একটি সংস্থার জন্য তথ্য একটি গুরুত্বপূর্ণ সম্পদ। সরকার, নাগরিক ও প্রতিষ্ঠানসমূহের মধ্যে আস্থা প্রতিষ্ঠা ও তাহা বজায় রাখিতে তথ্য সুরক্ষা অপরিহার্য। তথ্য নিরাপত্তা একটি সংস্থার জনবল ও প্রযুক্তির সহিত সংশ্লিষ্ট এমন একটি প্রক্রিয়া যাহার মাধ্যমে সেই সংস্থা তাহার তথ্যের সংরক্ষণ ও নিরাপত্তা বিধান করে। তথ্য নিরাপত্তা পলিসি তথ্যকে আক্রমণ বা হুমকি বা অপব্যবহার বা ক্ষতি বা অননুমোদিত প্রবেশাধিকার হইতে সুরক্ষার জন্য পলিসি ও নিয়ন্ত্রণ কৌশল নির্ধারণে সহায়তা করে।

(২) এই নির্দেশনাপত্রের (গাইডলাইন) উদ্দেশ্য হইল:

- ক. বাংলাদেশ সরকারের সংস্থাগুলিকে তথ্য নিরাপত্তার বিষয়বস্তু উপলব্ধি করিতে সহায়তা করা,
- খ. তথ্য নিরাপত্তা পলিসি প্রণয়ন করিতে পদ্ধতি নির্ধারণ করা,
- গ. তথ্য নিরাপত্তা পলিসি বাস্তবায়নে তাহাদিগকে যথাযথ নির্দেশনা প্রদান করা।

৬। গাইডলাইনের পরিধি

বাংলাদেশে যে সকল সরকারি, আধা-সরকারি, স্বায়ত্তশাসিত প্রতিষ্ঠান বা পাবলিক লিমিটেড কোম্পানি তাহাদের নিজস্ব তথ্য নিরাপত্তা পলিসি ডকুমেন্ট প্রণয়ন করিতে আগ্রহী তাহারা এই নির্দেশনাপত্র (গাইডলাইন) ব্যবহার করিতে পারিবে। তাহাদের তথ্য সুরক্ষার লক্ষ্যে পলিসি প্রণয়নে তাহাদের জন্য ইহা একটি সহায়ক দলিল। কোনো বেসরকারি প্রতিষ্ঠানও এই নির্দেশনাপত্র (গাইডলাইন) অনুসরণ করিতে পারিবে।

৭। তথ্য সম্পদ

(১) এই অনুচ্ছেদ কোনো সংস্থার গুরুত্বপূর্ণ সদস্যদের সংস্থার তথ্য বা উপাত্ত সম্পর্কে তাহাদের ধারণা পুনর্নির্মাণে সাহায্য করিবে। ইহা তাহাদিগকে স্ব স্ব ভূমিকা ও দায়িত্ব অনুসারে কিভাবে তথ্যের অবস্থাসমূহ নিরূপণ, তথ্য সম্পদ শ্রেণিকরণ, তথ্য সম্পদের মালিকানা ও তত্ত্বাবধায়ক নির্ধারণ এবং তথ্য কিভাবে সংরক্ষণ করিতে হইবে তাহা উপলব্ধি করিতে সাহায্য করিবে।

(২) তথ্যের সংজ্ঞা

প্রতিষ্ঠানের অন্যান্য গুরুত্বপূর্ণ সম্পদের মতো তথ্য এমন একটি সম্পদ যাহা প্রতিষ্ঠানের কার্যক্রমের জন্য অপরিহার্য এবং যাহা যথাযথ উপায়ে সুরক্ষিত থাকে। ব্যাপক অর্থে তথ্যবলিতে বুঝায় এমন ভিত্তি যাহার উপার নির্ভর করিয়া সংস্থা তাহাদের কার্যক্রম পরিচালনা করিয়া থাকে। নির্ভরযোগ্য তথ্য ভালো সিদ্ধান্ত গ্রহণে সহায়তা করিয়া প্রতিষ্ঠানের সক্ষমতা বৃদ্ধি করে। সরকার সেই সকল তথ্য সংরক্ষণ করে, যাহা কার্য বাস্তবায়নের ক্ষেত্রে প্রশাসনিক, রাজনৈতিক, বাণিজ্যিক কিংবা ব্যক্তিগত কারণে গুরুত্বপূর্ণ। অননুমোদিত বা আকস্মিক পরিবর্তন, ক্ষতি/বিনষ্ট বা অনাকাঙ্ক্ষিত প্রকাশ হইতে এই তথ্য রক্ষা করিবার জন্য সরকারের অন্যতম দায়িত্ব ও আইনগত বাধ্যবাধকতা রহিয়াছে। সঠিকভাবে তথ্য ব্যবহারের ক্ষেত্রে নৈতিকতার বিষয়টিও জড়িত।

(৩) তথ্যের বিভিন্ন রূপ হইতে পারে যাহা নিম্নরূপ :

- ক. প্রামাণ্য দলিল ও কাগজপত্র;
- খ. ইলেক্ট্রনিক উপাত্ত;
- গ. তথ্য ব্যবস্থাসমূহ (সফটওয়্যার, হার্ডওয়্যার ও নেটওয়ার্ক) যাহার মাধ্যমে তথ্য সংরক্ষণ, প্রক্রিয়াকরণ ও আদান প্রদান করা হয়;
- ঘ. ব্যক্তির বুদ্ধিবৃত্তিক তথ্য (জ্ঞান বা ধারণাসমূহ);
- ঙ. ভৌত উপকরণসমূহ (Physical items) যাহা হইতে তথ্যের ডিজাইন, উপাদান বা ব্যবহার সম্পর্কিত ধারণা পাওয়া যাইবে; এবং
- চ. ছবি, অডিও বা ভিডিও ক্লিপ।

(৪) তথ্য সম্পদের সংজ্ঞা

সম্পদ হইল এমন কিছু যাহা প্রতিষ্ঠান, সংস্থা বা দেশের জন্য মূল্যবান। একটি প্রতিষ্ঠানের জন্য তথ্য অত্যন্ত গুরুত্বপূর্ণ সম্পদ। সম্পদ যাহারা ব্যবহার করেন এবং যাহারা উহার সত্ত্বাধিকারী সেই সব স্টেকহোল্ডারদের মধ্যে আস্থা নিশ্চিতকরণের জন্য সম্পদকে সুরক্ষিত রাখিতে হইবে। নিরাপত্তাবিষয়ক ঝুঁকি নির্ধারণের সহিত সম্পদ সংরক্ষণ একান্তভাবে সম্পর্কিত। নিরাপত্তাবিষয়ক ঝুঁকি নির্ধারণে প্রথম কাজ হইল সংশ্লিষ্ট প্রতিষ্ঠানের তথ্য সম্পদের (যেমন: সংশ্লিষ্ট প্রতিষ্ঠানের কম্পিউটার ব্যবস্থায় সংরক্ষিত এপ্লিকেশন প্রোগ্রাম, সংরক্ষিত উপাত্ত, প্রতিবেদন, পণ্যের ডিজাইন ও স্পেসিফিকেশন, প্রস্তাব, কর্মপরিকল্পনা, আর্থিক দলিলাদি, উপাত্তভান্ডার (ডাটাবেইস) এবং অন্যান্য ফাইল ও দলিলপত্র) মজুদ সমীক্ষা করিয়া দেখা। সমীক্ষার উদ্দেশ্য হইল সম্পদসমূহ ও উহাদের পরিধি সম্পর্কে জানিতে সাহায্য করিবার লক্ষ্যে সেইগুলি পরিকল্পনা অনুযায়ী সুবিন্যস্ত করা। বিভিন্ন সম্পদের সঠিক সত্ত্বাধিকারী নির্ধারণ এবং তাহাদেরকে সম্পদের গুরুত্ব ও তাৎপর্য নির্ধারণের দায়িত্ব গ্রহণের জন্য উদ্বুদ্ধ করা প্রয়োজন।

(৫) সম্পদে কাহারো প্রবেশাধিকার পাইবে তাহা নির্ধারণের লক্ষ্যে সম্পদকে অবশ্যই শ্রেণিকরণ করিতে হইবে। তথ্য সম্পদ সঠিকভাবে চিহ্নিত এবং সঠিকভাবে শ্রেণিকৃত ও তাহাদের পরিধি নির্ধারিত হইলে পরবর্তী পদক্ষেপ হইবে কাহার কোন তথ্য প্রবেশাধিকার থাকিবে তাহা নির্ধারণ করা। অনেক ধরনের সম্পদ রহিয়াছে যাহা নিম্নরূপ (কিন্তু ইহাদের মধ্যে সীমাবদ্ধ নহে):

- ক. উপাত্তভান্ডার (ডাটাবেইস) ও ডাটা ফাইল চুক্তি পত্র, প্রসেস সহ System documentation, গবেষণা তথ্য, ব্যবহার-বিধি, প্রশিক্ষণ-উপকরণ, পরিচালনা বা সহায়ক পদ্ধতি (operational or support procedures), কার্যক্রমের ধারাবাহিকতা পরিকল্পনা (business continuity plans), অসুবিধার সম্মুখীন হইলে বিশেষ ব্যবস্থা চালুকরণ (fallback arrangements), অডিট বিবরণী এবং চূড়ান্তভাবে সংরক্ষিত তথ্য (archived information);
- খ. অ্যাপ্লিকেশন সফটওয়্যার, সিস্টেম সফটওয়্যার, সিস্টেম উন্নয়ন যন্ত্রাংশ এবং অন্যান্য জরুরী প্রয়োজনীয় সুবিধাদি;
- গ. কম্পিউটার সরঞ্জাম, কমিউনিকেশন সরঞ্জাম, স্থানান্তরযোগ্য প্রচার সরঞ্জাম ও অন্যান্য সরঞ্জাম;
- ঘ. হিসাব ও যোগাযোগ সেবা (Computing and Communication Services);
- ঙ. জনবল, তাহাদের যোগ্যতা, দক্ষতা ও অভিজ্ঞতা;
- চ. বস্তুগত নহে এমন সম্পদ যেমন প্রতিষ্ঠানের সুনাম ও ভাবমূর্তি।

(৬) কোন কার্যক্রম পরিচালনা বা বাস্তবায়নের সময় তথ্য সৃষ্টি, প্রক্রিয়াকরণ, জমাকরণ, সংরক্ষণ করা হয় বা ইহা মুছিয়া ফেলা হয়। সংরক্ষিত উপাত্তভান্ডার (database), চিঠিপত্র (mail), সোর্স কোড, দালিলিক কাগজপত্র, ডিজাইন, ই-মেইল, ডাটাবেস, প্রসেস ডাটা, ছবি ইত্যাদি ইহার উদাহরণ।

(৭) তথ্য সম্পদ হইল সুনির্দিষ্টভাবে সংজ্ঞায়িত করা যায় এবং যে কোনো মাধ্যমে সঞ্চিত করা যায় এমন তথ্য যাহা প্রতিষ্ঠানের জন্য 'মূল্যবান' বলিয়া স্বীকৃত। একটি প্রতিষ্ঠানের জন্য সবচেয়ে গুরুত্বপূর্ণ ও মূল্যবান তথ্য হইলো সেইগুলি যাহা ঐ সংস্থার মূল বা সর্বাধিক গুরুত্বপূর্ণ দায়িত্ব, সামর্থ্য বা লক্ষ্যমাত্রার সাথে সংশ্লিষ্ট। তথ্যের গোপনীয়তা, শুদ্ধতা ও সহজলভ্যতা ভঙ্গ হইলে প্রতিষ্ঠান কতখানি ক্ষতিগ্রস্ত হইবে তাহার মাধ্যমে বুঝা যায় ঐ প্রতিষ্ঠানে তথ্য সম্পদের কতখানি মূল্য। প্রতিষ্ঠানের সম্ভাব্য ক্ষতিসমূহের মধ্যে রহিয়াছে-প্রত্যক্ষ ও পরোক্ষ আর্থিক ক্ষতি (তাৎক্ষণিক বা পরবর্তী), রাজস্ব ঘাটতি, সেবা প্রদানবিষয়ক বাধ্যবাধকতা পূরণে ব্যর্থতা বা সুনাম হানি। নিরাপত্তা বিধানে ব্যর্থতার পরোক্ষ ফলাফলও বিবেচনা করিতে হইবে। তথ্য সম্পদের মূল্য নিরূপণের ভিত্তি হইলঃ

- ক. তথ্য সম্পদের গোপনীয়তা (Confidentiality);
- খ. তথ্য সম্পদের শুদ্ধতা; (Integrity)

- গ. তথ্য সম্পদের প্রামাণ্যতা (Authenticity);
- ঘ. অনস্বীকৃতি (non-repudiation); এবং
- ঙ. তথ্য সম্পদের সহজলভ্যতা (Availability)।

(৮) তথ্যের বিভিন্ন রূপ

পূর্বে উল্লেখ করা হইয়াছে যে, তথ্যের বিভিন্ন রূপ রহিয়াছে। ইহার অবস্থাও বিভিন্ন। তথ্য নিরাপত্তাবিষয়ক পলিসি উন্নয়নকালে সংস্থার জন্য ঐ সকল অবস্থা বিবেচনা করা খুবই জরুরি। তথ্যের সাধারণ অবস্থাসমূহ হইল:

- ক. তথ্য যাহা চূড়ান্তভাবে সংরক্ষণ করা হইয়াছে (archived) (পুরানো দিনের ক্রমপুঞ্জিভূত)
- খ. সংস্থার একান্ত নিজস্ব তথ্য বা জনবলের তথ্য যাহা ডেটাবেস (database) বা টেপ-ড্রাইভ বা অন্য কোনো মিডিয়ায় সঞ্চিত থাকে;
- গ. এপ্লিকেশন দ্বারা প্রক্রিয়াকরণকৃত দৈনন্দিন কার্যক্রমবিষয়ক তথ্য;
- ঘ. সংস্থার ওয়েবসাইট-এ প্রদত্ত স্ট্যাটিক ও ডাইনামিক তথ্য;
- ঙ. যোগাযোগ/চিঠিপত্র লেনদেন, উপলব্ধি ও জ্ঞান;
- চ. তথ্য যাহা সংস্থা/সরকারের ইন্ট্রানেট-এ প্রক্রিয়াকরণকৃত;
- ছ. তথ্য যাহা সংস্থা/সরকারের ইন্ট্রানেট-এ প্রক্রিয়াকরণকৃত;
- জ. তথ্য যাহা এক্সট্রানেট-এ প্রক্রিয়াকরণকৃত।

(৯) তথ্যের বিভিন্ন প্রকার অবস্থার জন্য বিভিন্ন ধরনের নিরাপত্তা কৌশল প্রয়োজন। তথ্যের গুরুত্ব বিবেচনা করিয়া ও প্রয়োজন অনুসারে তথ্যের শ্রেণিকরণ করিয়া ইহা করিতে হইবে। তথ্যের গুরুত্বের ভিত্তিতে একই ধরনের তথ্যের জন্য নিরাপত্তা নিয়ন্ত্রণ আরোপ করা খুবই সহজ ও সুবিধাজনক। প্রত্যেক সংস্থাকে তাহার তথ্যের অবস্থা নির্ণয় করিয়া শ্রেণিকরণকৃত তথ্যের সহিত সামঞ্জস্য রাখিয়া নিরাপত্তা পলিসি নিরূপণ করিতে হইবে।

(১০) তথ্যের শ্রেণিকরণ

বিভিন্ন পদ্ধতিতে বিভিন্ন ধরনের তথ্যের নিরাপত্তা বিধান করিতে হইবে। সুতরাং একটি শ্রেণিকরণ পদ্ধতি প্রয়োজন যাহার দ্বারা শ্রেণিকরণ করা হইবে। শ্রেণি অনুসারে কিভাবে তথ্য ব্যবহার করিতে হইবে সেই বিষয়ে একটি পলিসি প্রণয়ন করিতে হইবে এবং তদানুযায়ী তথ্য ব্যবহারবিষয়ক নিরাপত্তা কৌশল প্রয়োগ করা হইবে। তথ্য শ্রেণিকরণের ফলে সঠিক মাত্রায় তথ্যের সুরক্ষা নিশ্চিত হয়। তথ্যের প্রয়োজনীয়তা, অধিকার ও তথ্য ব্যবহারে প্রত্যাশিত সুরক্ষা প্রদানের বিষয় নির্দেশ করিবার জন্য তথ্য শ্রেণিকরণ করিতে হইবে। তথ্যের মধ্যে স্পর্শকাতরতা ও গুরুত্বের বিভিন্ন মাত্রা রহিয়াছে। কিছু কিছু তথ্যের অধিক মাত্রার সুরক্ষা বা সতর্কতার সাথে ব্যবহারের প্রয়োজন হইতে পারে। যথাযথ নিরাপত্তা স্তর নির্ধারণ এবং তদানুযায়ী সতর্কতার সাথে ব্যবহারের প্রয়োজনীয়তা সংশ্লিষ্টদের অবহিত করিতে তথ্যের শ্রেণিকরণ পদ্ধতি ব্যবহার করিতে হইবে।

(১১) দেশ বা সংস্থার নিকট তথ্যের মূল্যমান, আইনগত প্রয়োজন, স্পর্শকাতরতা ও গুরুত্ব অনুসারে তথ্যের শ্রেণিকরণ করা যাইতে পারে। দেশ ও সংস্থা ভেদে শ্রেণিকরণ পদ্ধতির মধ্যে ভিন্নতা রহিয়াছে। অধিকাংশ দেশে সাধারণত নিম্নোক্ত পাঁচটি শ্রেণিতে তথ্যকে বিভক্ত করা হয়;

- ক. সর্বোচ্চ গোপনীয় (Top Secret)
- খ. একান্ত গোপনীয় (Secret)
- গ. গোপনীয় (Confidential)
- ঘ. সীমিত (Restricted)
- ঙ. উন্মুক্ত বা অশ্রেণিকরণকৃত (Public or Unclassified)

(১২) তথ্যসম্পদ শ্রেণিকরণ করিবার সময় ইহা সরকারি আইন ও বিধিবিধানের সহিত সঙ্গতিপূর্ণ কিনা তাহা দেখিয়া লইতে হইবে। কোন সংস্থা তাহাদের নিজস্ব প্রয়োজনে কম বা বেশি স্তর বিশিষ্ট শ্রেণিবিন্যাস পদ্ধতি অনুসরণ করিতে পারে। তবে সংস্থার জন্য সর্বাধিক গুরুত্বপূর্ণ কাজ হইল তাহাদের নিজেদের তথ্য বিশ্লেষণ করিয়া তথ্যের অবস্থা ও শ্রেণিবিন্যাস নিরূপণ করা। শ্রেণিবিন্যাস অনুযায়ী সংস্থা তথ্য সম্পদের উপর নিরাপত্তা নিয়ন্ত্রণ আরোপ করিবে।

(১৩) তথ্যের সত্ত্বাধিকারী

তথ্যের সত্ত্বাধিকারী হইলেন এমন একজন ব্যক্তি বিভিন্ন অবস্থার ভিত্তিতে তথ্যের শ্রেণিকরণের জন্য দায়িত্ব প্রাপ্ত এবং যার তথ্যের গোপনীয়তা, শুদ্ধতা, প্রামাণ্যতা ও লভ্যতা রক্ষার উপর কার্যকর নিয়ন্ত্রণ রহিয়াছে। তথ্যের সত্ত্বাধিকারীর উপর তথ্য সৃষ্টি, উন্নয়ন, রক্ষণাবেক্ষণ করিবার; তথ্য সম্পদের উপর নিরাপত্তা নিয়ন্ত্রণ আরোপ করিবার; যথাযথ পর্যায়ের সুরক্ষা ব্যবস্থা আরোপ করিবার দায়িত্ব থাকিবে। সেই সাথে আর্থিক ব্যয় ও সুফল লাভের দিক বিবেচনায় আনিয়া প্রতিষ্ঠানের মূল উদ্দেশ্য ও লক্ষ্য বাস্তবায়ন নিশ্চিত করিতে সময়ে সময়ে তথ্যের শ্রেণিকরণ, নিরাপত্তা নিয়ন্ত্রণ, পর্যায়ক্রমিক প্রবেশাধিকার সীমিতকরণের বিষয়সমূহ পুনর্বিবেচনা করিবার জন্য তাহার কর্তৃত্ব ও দায়িত্ব থাকিবে।

(১৪) তথ্যের সংরক্ষক

তথ্যের সংরক্ষক হইলেন তথ্যের সত্ত্বাধিকারী কর্তৃক নিয়োজিত এমন একজন ব্যক্তি যিনি সত্ত্বাধিকারী কর্তৃক প্রবর্তিত রক্ষণাবেক্ষণ ও নিয়ন্ত্রণ ব্যবস্থা অনুসরণ করিয়া তথ্য সুরক্ষা করিবেন। তিনি অন্যদেরকে তথ্য প্রদান করিবার প্রয়োজন হইলে সে বিষয়ে সত্ত্বাধিকারী কর্তৃক দায়িত্বপ্রাপ্ত হইবেন। সংরক্ষক তথ্যের সত্ত্বাধিকারী কর্তৃক নির্ধারিত উপায়ে নিয়মিত ব্যাকআপ (Backup) ও উপাত্তের গ্রহণযোগ্যতা (validity) যাচাই কার্যক্রম সম্পন্ন এবং ব্যাকআপ (Backup) হইতে বিভিন্ন উপায়ে উপাত্ত নতুন ভাবে সংরক্ষণ করিবেন ও তথ্যে প্রবেশাধিকারে নিয়ন্ত্রণ আরোপ করিবারও দায়িত্ব পালন করিবেন। প্রতিটি তথ্যসম্পদ একজন সংরক্ষকের দায়িত্বে থাকিবে। সংরক্ষককে তথ্য সম্পদের নিরাপত্তার জন্য চূড়ান্তভাবে দায়িত্বশীল থাকিতে হয়। সেই জন্য তাহাকে নিশ্চিত হইতে হয় যে সকল দায়িত্ব যথাযথভাবে সম্পন্ন হইতেছে।

(১৫) দায়িত্ব ও কর্তব্য

সংস্থাসমূহ তাহাদের আওতায় থাকা তথ্য সম্পদসমূহের যথাযথ নিরাপত্তার জন্য দায়িত্বশীল থাকিবে। সংস্থাসমূহ সবচেয়ে ভাল রুবিতে পারে যে তাহাদের তথ্য-সম্পদসমূহের গুরুত্ব কি, ইহার মূল্য কিরূপ এবং ইহার প্রতি কি ঝুঁকি আছে এবং তাহা সুরক্ষার জন্য উপযুক্ত পদক্ষেপ কি। তাই প্রতিষ্ঠানকে তাহাদের তথ্য সম্পদের যথাযথ নিরাপত্তা সুনিশ্চিত করিতে হইবে। এই লক্ষ্য অর্জন করিতে হইলে সকল তথ্যসম্পদের বিবরণসহ একজন নির্ধারিত সত্ত্বাধিকারী থাকিতে হইবে। সত্ত্বাধিকারীদেরকে তথ্য

নিরাপত্তা ব্যবস্থা নিয়ন্ত্রণের দায়িত্ব প্রদান করিতে হইবে। তথ্য সম্পদের সত্ত্বাধিকারীর তথ্য/সম্পদের শ্রেণিকরণ নির্ধারণ, সময়ে সময়ে উহা পরীক্ষা-নিরীক্ষা করিবার এবং উহা হালনাগাদ করা হইয়াছে কিনা ও উহা যথাযথ পর্যায়ে নিরাপত্তা নিয়ন্ত্রণের ভিতরে রহিয়াছে কিনা তাহা নিশ্চিত করিবার দায়িত্ব থাকিবে। যথাবিহীন বিবেচিত হইলে সুনির্দিষ্ট কোনো দায়িত্ব অন্যকে দেওয়া যাইতে পারে, তবে তথ্য সম্পদের সঠিক সুরক্ষার দায়িত্ব সত্ত্বাধিকারী সার্বিকভাবে পালন করিবেন। কোনো সংস্থার অত্যন্ত গুরুত্বপূর্ণ বাধ্যতাবাহকতা হইল তাহাদের তথ্যের দায়িত্ব বাহিরের কাহারও উপর প্রদান না করা অর্থাৎ তথ্য সম্পদের নিরাপত্তার দায়িত্ব সর্বদা যে সংস্থার তথ্য তাহার ভিতরেই থাকিবে।

(১৬) তথ্য সম্পদ সংরক্ষণ (Archiving)

ক্রমাগত সঞ্চয়নের ফলে তথ্য ভান্ডার বিশাল আকার ধারণ করিতে পারে এবং ইহা তথ্যের সর্বোত্তম ব্যবহারে বাধা সৃষ্টি করিতে পারে। এ কারণে ব্যবহার উপযোগিতা-উল্লীর্ণ, একাধিক কপি, অতিরিক্ত এবং অপ্রয়োজনীয় তথ্য হয় বিনষ্ট নতুবা চূড়ান্ত সংরক্ষণ করা যাইতে পারে। কোন সংস্থার তথ্য নষ্ট করিতে হইলে তথ্যের সত্ত্বাধিকারী এবং তথ্য সংরক্ষককের যথাযথ অনুমোদন গ্রহণ করিতে হইবে এবং তাহাদের সংরক্ষিত লগ বইয়ে নষ্ট করিবার কারণ লিপিবদ্ধ করিতে হইবে। সংরক্ষণের ক্ষেত্রে একটি সংস্থা কাগজ এবং নথিপত্র সংরক্ষণের মতো অবশ্যই ইলেকট্রনিক তথ্য সম্পদ সংরক্ষণের বিষয় বিবেচনা করিবে। তথ্য সম্পদের গুরুত্ব বিবেচনা করিয়া একটি সংস্থা উহার তথ্য সম্পদ সংরক্ষণের মেয়াদ নির্ধারণ করিবে। মেয়াদ নির্ধারণের ক্ষেত্রে সংস্থাকে অবশ্যই তথ্য ও যোগাযোগ প্রযুক্তি আইন-২০০৬ এর ৯ নম্বর ধারা এবং অন্যান্য প্রাসঙ্গিক আইন অনুসরণ করিতে হইবে।

(১৭) অনুচ্ছেদ অনুযায়ী করণীয়

অনুচ্ছেদ ৭ এ বর্ণিত কাজগুলি একটি সংস্থার তথ্য নিরাপত্তা পলিসি যথাযথভাবে বিন্যস্ত করার প্রারম্ভিক কাজ। সামগ্রিকভাবে ইহাকে তথ্য সংগ্রহ ও তথ্য সম্পদ ব্যবস্থাপনা বলা হয়। ইহা সম্পন্ন করিতে গৃহিতব্য পদক্ষেপগুলি নিম্নরূপঃ

(ক) তথ্য শ্রেণিকরণ ও উহার অবস্থা

তথ্যের মূল্য, আইনগত প্রয়োজনীয়তা, স্পর্শকাতরতা ও সংস্থার জন্য গুরুত্বের বিবেচনায় উহার বিশ্লেষণ ও শ্রেণিকরণ করা আবশ্যিক। অতঃপর শ্রেণিকরণকৃত তথ্যের অবস্থাও নির্ণয় করিতে হইবে।

(খ) তথ্য সম্পদের ইনভেন্টরি (inventory)

সকল তথ্য সম্পদ সনাক্ত করিতে হইবে এবং উহার একটি ইনভেন্টরি তৈরী ও রক্ষণাবেক্ষণ করিতে হইবে। সনাক্তকৃত সকল তথ্য সম্পদের গুরুত্ব লিপিবদ্ধ করিতে হইবে। যে কোন ধরনের বিপর্যয় হইতে তথ্য সম্পদ পুনরুদ্ধার করিবার জন্য তথ্য সম্পদের ইনভেন্টরিতে সম্পদের ধরণ, আকার, অবস্থান, ব্যাকাআপ সম্পর্কিত তথ্য, লাইসেন্স বিষয়ক তথ্য এবং প্রতিষ্ঠানের কাছে ইহার প্রয়োজনীয়তা-মূল্যসহ অন্যান্য সকল তথ্য অন্তর্ভুক্ত থাকিবে। তথ্য সম্পদের এই ইনভেন্টরি অন্য ইনভেন্টরিসমূহের প্রতিরূপ হইবে না, তবে অন্যগুলির সহিত সামঞ্জস্যপূর্ণ হইতে হইবে।

(গ) তথ্য সনাক্তকরণ চিহ্ন ও ব্যবহার

সংস্থা কর্তৃক গৃহীত তথ্য শ্রেণিকরণ পদ্ধতি অনুসরণে তথ্য সনাক্তকরণ ও ব্যবহারের জন্য একটি উপযুক্ত পদ্ধতি উন্নয়ন ও বাস্তবায়ন করিতে হইবে। এই পদ্ধতির মধ্যে ভৌত ও ইলেকট্রনিক আকারে বিদ্যমান তথ্য সনাক্তকরণের ব্যবস্থা অন্তর্ভুক্ত থাকিতে হইবে।

(ঘ) তথ্য সম্পদের সত্ত্বাধিকার

তথ্য প্রক্রিয়াকরণ ব্যবস্থার সহিত সম্পর্কিত সকল তথ্য ও সম্পদ সংস্থার সুনির্দিষ্ট কোন অংশের মালিকানাধীন থাকিতে হইবে। তথ্য সম্পদের সত্ত্বাধিকারী নিম্নোক্ত বিষয়ে দায়িত্বশীল থাকিবেন;

- (ক) তথ্য প্রক্রিয়াকরণ ব্যবস্থার সহিত সম্পর্কিত তথ্য ও সম্পদ যথাযথভাবে শ্রেণীকরণ নিশ্চিত করিতে হইবে;
- (খ) প্রবেশাধিকার নিয়ন্ত্রণ পলিসি বিবেচনা করিয়া প্রবেশাধিকারের বাধ্যবাধকতা ও শ্রেণীকরণ নির্ধারণ ও মাঝে মাঝে পর্যালোচনা করিতে হইবে;

(ঙ) তথ্য সম্পদের গ্রহণযোগ্য ব্যবহার

তথ্য প্রক্রিয়াকরণ ব্যবস্থার সহিত সম্পর্কিত তথ্য সম্পদের গ্রহণযোগ্য ব্যবহার বিধি নির্ধারণ লিপিবদ্ধকরণ ও বাস্তবায়ন করিতে হইবে। সকল কর্মচারী, ঠিকাদার ও অন্যান্য ব্যবহারকারীগণ এই ব্যবহার বিধি অনুসরণ করিবেন।

(চ) দায়িত্বাবলী

তথ্যের সত্ত্বাধিকারী, সংরক্ষণ ও অন্যান্য ব্যবহারকারী নির্ধারণ করিতে হইবে এবং তাহাদের মধ্যে তথ্য সম্পদ ব্যবস্থাপনার দায়-দায়িত্ব নির্দিষ্ট করিয়া দিতে হইবে। তথ্য সম্পদের সুরক্ষার লক্ষ্যে তাহাদের দায়-দায়িত্ব স্পষ্টরূপে নির্ধারণ করিতে হইবে এবং তাহা মাঝে মাঝে পর্যালোচনা করিতে হইবে। এ সকল বিষয়াদি নির্ধারণের ক্ষেত্রে তথ্য সম্পদ সংরক্ষণ এবং সংরক্ষণ মেয়াদও বিবেচনা করিতে হইবে।

৮। তথ্য নিরাপত্তা কৌশল

(১) তথ্য নিরাপত্তা পলিসি প্রণয়নের পূর্বে বিভিন্ন সংস্থাকে তথ্য নিরাপত্তা হুমকি হইতে নিরাপত্তার লক্ষ্যে প্রক্রিয়া, জনবল, প্রযুক্তি, পদ্ধতিসমূহের সমন্বয় সাধনে পরিকল্পনা গ্রহণ করিতে হইবে। তথ্য নিরাপত্তা সম্পর্কিত নূতন নূতন হুমকি ও অরক্ষিত অবস্থা নিরসনের লক্ষ্যে মাঝে মাঝে কৌশলসমূহ পুনঃনিরীক্ষা করিয়া দেখিতে হইবে। এই অনুচ্ছেদটি তথ্য নিরাপত্তা কৌশল সংক্রান্ত বিশ্বের সর্বোত্তম পদ্ধতিসমূহ জানিতে এবং সংস্থার প্রয়োজন অনুযায়ী অনুশীলনযোগ্য সর্বোত্তম পদ্ধতি গ্রহণ করিতে সহায়তা প্রদান করিবে।

(২) কৌশল প্রণয়ন

নিজস্ব কৌশল প্রণয়নের জন্যে সর্বোত্তম অনুশীলনসমূহ সম্পর্কে জানা প্রয়োজন তবে সবসময় কেবল সর্বোত্তম অনুশীলনগুলো গ্রহণ করা যৌক্তিক বিবেচিত নাও হইতে পারে। একমাত্র সর্বোত্তম অনুশীলনসমূহ গ্রহণের ফলে গৃহীত কৌশলটি অকার্যকর ও অবাস্তব হয়ে পরিতে পারে। সুতরাং সংশ্লিষ্ট সংস্থার বাস্তব অবস্থা ও প্রচলিত সর্বোত্তম পদ্ধতিসমূহের সংমিশ্রনে কৌশল প্রণয়নের উপর গুরুত্বারোপ করা হইয়া থাকে। তথ্য নিরাপত্তা কৌশল প্রণয়নে নিম্নোক্ত পর্যায়সমূহ অনুসরণ করা হয়ঃ

(ক) পর্যায়-১ঃ উদ্দেশ্য

তথ্য নিরাপত্তা কৌশল গ্রহণ করিতে হইলে কোন প্রতিষ্ঠান/সংস্থা'র একটি উদ্দেশ্য থাকিতে হইবে। অধিকাংশ প্রতিষ্ঠান/সংস্থা'র উদ্দেশ্য হইতেছে সাইবার স্পেসে হামলা হইতে তাহাদের তথ্যের সুরক্ষা প্রদান করা। তথ্য চুরি বা ক্ষতির হুমকি সংস্থার লক্ষ্য ও কার্যকারিতাকে ব্যাহত করিতে পারে। সুতরাং হুমকি হইতে তথ্য সুরক্ষা করিত হইলে প্রতিষ্ঠানসমূহকে তাহাদের লক্ষ্য ও উদ্দেশ্য স্থির করিত হইবে।

(খ) পর্যায়-২ঃ উপলব্ধি

কোন সংস্থার নিরাপত্তা নীতি প্রণয়নের পূর্বে সেই সংস্থা সম্পর্কে পরিপূর্ণ ধারণা থাকা আবশ্যিক। সংস্থার লক্ষ্য ও উদ্দেশ্যসমূহ বিবেচনায় আনাও জরুরী। যে সকল নীতিসমূহ প্রণয়ন করা হইবে উহাদের সাথে সংস্থার বর্তমান নীতি, বিধি, প্রবিধান ও আইনের সামঞ্জস্যতা থাকা বাঞ্ছনীয়। নীতি প্রণীত হওয়ার পূর্ব পর্যায়ে-তথ্য সম্পদ এবং উহার সহিত সম্পর্কিত ঝুঁকি, দুর্বল দিকগুলো ও হুমকিসমূহ চিহ্নিতকরণ, সন্নিহিত ব্যয় ও ঝুঁকি প্রশমনের শতকরা হার উল্লেখ করিয়া সম্ভাব্য প্রতিরক্ষা ও নিয়ন্ত্রণসমূহ চিহ্নিতকরণ এবং দায়িত্ব ও কর্তব্যসমূহ পুণঃনির্ধারণ সম্পর্কিত তথ্য সংগ্রহ করাও জরুরী।

(গ) পর্যায়-৩ঃ পরিকল্পনা

উপানুচ্ছেদ (৪) অনুসরণপূর্বক সংগৃহীত তথ্য এবং সংশ্লিষ্ট সংস্থার লক্ষ্য ও উদ্দেশ্য বিবেচনা করতঃ এই পর্যায়ে নিরাপত্তা নীতি প্রণয়ন করিতে হইবে। এই পর্যায়ে প্রণীতব্য নীতি 'র সাথে বিধিবদ্ধ প্রণালী, মানদণ্ড গাইডলাইন ইত্যাদিও অন্তর্ভুক্ত হইবে। নিরাপত্তা নীতি প্রণয়নকালে সংস্থাকে ISO/IEC 27002: Code of Practice for Information Security Management হইতে সাহায্য ও মানদণ্ড যাচাই করিয়া লওয়া যাইতে পারে। একইভাবে নীতি সংকলনকালে সংস্থাকে তাহাদের তথ্য সম্পদের অবস্থান নির্ধারণ এবং ইহা তাহাদের নিজস্ব আওতাভুক্ত থাকিবে নাকি বাহিরে থাকিবে তাহা নির্ধারণ করিয়া লইতে হইবে। সরকারী সংস্থাসমূহ অবশ্যই তাহাদের তথ্য সম্পদসমূহ দেশের অভ্যন্তরে রাখা নিশ্চিত করিবেন। বাংলাদেশ কম্পিউটার কাউন্সিলে রক্ষিত জাতীয় ডাটা সেন্টারে সরকারী সংস্থাসমূহের তথ্য সংরক্ষণের জন্য পরামর্শ দেওয়া হইল। নীতিসমূহ বলবৎকরণের পূর্বে প্রয়োগকারী সংস্থা এবং ব্যবহারকারীগণের সাথে পরামর্শ করা যাইতে পারে। এ ধরনের পরামর্শের ফলে একটি কার্যকরী নিরাপত্তা নীতি প্রণয়ন সহজ হইবে।

(ঘ) পর্যায়-৪ঃ বাস্তবায়ন

পলিসি ও অন্যান্য প্রাসঙ্গিক পদ্ধতিসমূহ বা নির্দেশনাপত্র প্রণয়নের পর সংস্থা অবশ্যই তাহার জনবলকে প্রশিক্ষিত করিবে এবং উক্ত নীতিসমূহ বাস্তবায়নকারীদের (ব্যবস্থাপনা কর্তৃপক্ষ, পরিচালনা পর্যদ, কর্মচারীবৃন্দ প্রমুখ) মধ্যে বিতরণ করিবে এবং এই মর্মে তাহাদের সাথে ঐক্যমতে পৌছাইবেন যে, বাস্তবায়নকারীগণ ঐ নীতিসমূহ সম্পূর্ণভাবে অনুধাবন করিয়াছেন এবং উহা মানিয়া চলিতে সম্মত আছেন। নিরাপত্তা নীতি গ্রহণ ও তা অনুসরণ করার মূল চাবিকাঠিই হইল শিক্ষা নিরাপত্তার প্রয়োজনে জনবলকে প্রশিক্ষিত করা এবং নীতি সংকলন প্রক্রিয়ায় তাহাদেরকে সম্পৃক্ত করা গুরুত্বপূর্ণ এই জন্যে যে, ইহা তাহাদেরকে পলিসি এড়াইয়া চলা এবং তাহার ফলে পলিসি অকার্যকর হওয়া থেকে বিরত রাখিবে। সেমিনার ও সচেতনতা বৃদ্ধি সংক্রান্ত প্রচারাভিযান গুলো তথ্য নিরাপত্তার বিশেষতঃ এর পাসওয়ার্ড নির্বাচন, স্ক্রিন লকিং, দলিল চিহ্নিতকরণ এবং ভৌত নিরাপত্তার তাৎপর্য অনুধাবনে সাহায্য করে। এছাড়া একটি সার্থক বাস্তবায়নের জন্য প্রারম্ভিক পর্যায়ে সহায়তা ডেস্কও চালু করা যাইতে পারে।

(ঙ) পর্যায়-৫ঃ মান্যতা যাচাই

কোন সংস্থা এমন একটি পদ্ধতি উদ্ভাবন করিবে যাহার মাধ্যমে সেখানকার নীতিসমূহ কতটুকু অনুসরণ করা হইতেছে তা পরিমাপ করা যাইবে এবং একটি নির্দিষ্ট মেয়াদান্তে এ ধরনের মান্যতা যাচাই করিবে। বলবৎকৃত নীতিসমূহের সফল বাস্তবায়ন নিশ্চিত করিতে একটি নিরীক্ষা দল গঠন করার বিষয়টি উপযুক্ত পদ্ধতির অন্তর্ভুক্ত হইতে পারে। নিরাপত্তা নীতিসমূহের মান্যতা পরিবীক্ষণের জন্য দায়িত্বপ্রাপ্ত নিরীক্ষকগণ ঐ নীতি বাস্তবায়নকারীদের হইতে স্বতন্ত্র হইবেন। নীতিসমূহ কঠোরভাবে বাস্তবায়ন করিতে হইবে এবং অমান্যতার ক্ষেত্রে শাস্তির বিধান থাকিতে হইবে।

(চ) পর্যায়-৬ঃ পরিবীক্ষণ ও মূল্যায়ন

সময়ের ব্যবধানে নূতন নূতন হুমকির আবির্ভাব হয় বলিয়া ভবিষ্যতে তথ্য ব্যবস্থাপনা উন্নয়নের জন্য একটি মূল্যায়ন ও পরিবীক্ষণ কৌশল অবলম্বন করা জরুরী। প্রতিষ্ঠানের পরিবর্তনের সাথে সাথে যে নূতন নূতন হুমকির সৃষ্টি হয় সেটাও মূল্যায়ন ও পরিবীক্ষণে কৌশলের অন্তর্ভুক্ত। নূতন সৃষ্ট কোন হুমকি প্রশাসনের জন্য নিরাপত্তার নিয়ন্ত্রণসমূহে প্রয়োজনে পরিবর্তন করিতে হইবে। কর্মদক্ষতার উন্নয়নের জন্য দরকার হইলে প্রশিক্ষণের মত গুরুত্বপূর্ণ বিষয়ের আয়োজন করা যাইতে পারে। সময়ের সাথে তাল মিলিয়ে নিরাপত্তা নীতিসমূহের প্রাসঙ্গিকতা বজায় রাখা অত্যন্ত জরুরী। প্রয়োজনে নূতন নূতন নীতি অন্তর্ভুক্ত করা যাইতে পারে।

(৩) অনুচ্ছেদ অনুযায়ী করণীয়

এই অনুচ্ছেদে নিরাপত্তা নীতি সংক্রান্ত কৌশলসমূহ বর্ণনা করা হইয়াছে। কার্যকরভাবে তথ্য সম্পদের সুরক্ষা দেবার লক্ষ্যে তথ্য নিরাপত্তা নীতিসমূহ প্রণয়ন করা একটি সংস্থার সারা জীবনব্যাপী কাজ। বিভিন্ন ধরনের হুমকি হইতে মূল্যবান তথ্যসম্পদের নিরাপত্তা প্রদানের জন্য সংস্থাসমূহ কর্তৃক অবশ্যই এই অনুচ্ছেদে বর্ণিত ধাপগুলো অনুসরণ করিতে হইবে। অনুচ্ছেদ ৭.৯ এ বর্ণিত করণীয় বিষয়সমূহ পূর্বে বর্ণিত কৌশলগুলোর ধাপসমূহেরই অংশবিশেষ। এই নির্দেশিকা পত্রটি ব্যবহারকারীদের কোন কাজটি আগে করিতে হবে সে বিষয়ে বিভ্রান্ত না হওয়ার জন্য সতর্ক থাকিতে হইবে। যাহারা কোন সংস্থার জন্য তথ্য নিরাপত্তা নীতি প্রণয়ন করিতে চাহেন, তাহারা ৮.১ অনুচ্ছেদে বর্ণিত ধাপসমূহ হইতে শুরু করিবেন। অন্যান্য অনুচ্ছেদগুলো এই ৬ (ছয়) টি ধাপ সম্পন্ন করিতে সাহায্য করিবে।

৯। ঝুঁকি, হুমকি ও অরক্ষিত অবস্থা

(১) নিরাপত্তা পলিসি প্রণয়নের সময় প্রত্যেক প্রতিষ্ঠান বা সংস্থাকে সম্ভাব্য এমন সকল ঝুঁকির বিষয়ে সতর্ক থাকিতে হইবে যাহা তাহাদের তথ্য সম্পদের নিরাপত্তা বিঘ্নিত করিতে পারে। তাহাদের তথ্য সম্পদ নষ্ট করিয়া দিতে পারে এমন হুমকি ও অরক্ষিত অবস্থা সম্পর্কেও প্রতিষ্ঠান বা সংস্থার স্পষ্ট ধারণা থাকিতে হইবে। তথ্য সম্পদের যথাযথ সংরক্ষণের জন্য ঝুঁকি, হুমকি ও অরক্ষিত অবস্থা সম্পর্কে সুস্পষ্ট ধারণা অপরিহার্য। এই অনুচ্ছেদ সংস্থাকে হুমকি, ঝুঁকি ও অরক্ষিত অবস্থা সম্পর্কে জানিতে এবং উহা চিহ্নিত ও বিশ্লেষণ করিতে সাহায্য করিবে।

২। ঝুঁকি, হুমকি ও অরক্ষিত অবস্থা সম্পর্কে ধারণা**(ক) ঝুঁকিঃ**

কোনো অরক্ষিত অবস্থা থাকার সুযোগে উদ্ভূত হুমকি হইতে তথ্য সম্পদ হারানো, ক্ষতি বা ধ্বংসের সম্ভাবনা (হইতে পারে আবার নাও হইতে পারে)। ঝুঁকি হ্রাসের জন্য ঝুঁকি চিহ্নিতকরণ এবং মাঝে মাঝে ঝুঁকি ব্যবস্থাপনা প্রক্রিয়াকরণ করা প্রয়োজন। সংস্থাকে তাহাদের তথ্য সম্পদের সম্ভাব্য ক্ষতি সাধন করিতে পারে এমন বড় বড় ঝুঁকি সম্পর্কে অবহিত থাকিতে হইবে। বড় বড় ঝুঁকি/দুর্বলতার কারণসমূহ হইলঃ

- ক. নিরাপত্তা নিশ্চিতকরণের জন্য অপরিপূর্ণ ব্যবস্থা
- খ. তথ্য শ্রেণিকরণকৃত না থাকা

- গ. অসম্পূর্ণ তথ্য নিরাপত্তা পলিসির অনুসরণ
- ঘ. নিরাপত্তা সতর্কতার অভাব
- ঙ. তথ্য ব্যবস্থায় দুর্বল প্রবেশাধিকার নিয়ন্ত্রণ
- চ. দাণ্ডরিক কোনো পলিসি না থাকা এবং পরিবীক্ষণ (Monitoring)/অনুপ্রবেশ অনুসন্ধানকারী বা ইন্সিডেন্ট মোকাবিলার জন্য টিম না থাকা
- ছ. পরিচালনা কার্যক্রম (Operating procedures) লিপিবদ্ধ না থাকা
- জ. কর্মচারীবৃন্দ পর্যাপ্তভাবে পরিচিতি না থাকা এবং পরিদর্শনকারীদের বাধাহীন বিচরণের সুযোগ থাকা
- ঝ. ভূমিকম্পপ্রবণ এলাকায় ভবন অবস্থিত হওয়া
- ঞ. ভবন বন্যাপ্রবণ এলাকায় অবস্থিত হওয়া কিংবা পানি নিষ্কাশন ব্যবস্থা না থাকায় সৃষ্ট বন্যায় ক্ষতিগ্রস্ত হওয়ার সম্ভাবনা থাকা
- ট. অগ্নি প্রতিরোধক ব্যবস্থা না থাকা, ইত্যাদি।

(খ) হুমকিঃ

হুমকি এমন কোনো অনাকাঙ্ক্ষিত ইন্সিডেন্টের সম্ভাব্য কারণ যাহা কোন সিস্টেম-এর বা প্রতিষ্ঠানের তথ্য সম্পদের ক্ষতি সাধনকরিতে পারে। হুমকি এমন কিছু যাহা উদ্দেশ্যমূলকভাবে বা আকস্মিকভাবে অরক্ষিত ব্যবস্থার সুযোগ গ্রহণ করিয়া সম্পদ নষ্ট বা ধ্বংস করিতে পারে। প্রাকৃতিক বিপর্যয়ের কারণে বা সংস্থার ভিতরে কিংবা বাহিরের উদ্দেশ্যমূলক বা আকস্মিক কর্মকাণ্ডের ফলে হুমকির সৃষ্টি হয়। তথ্য সম্পদে বা তাহাদের সহায়ক অবকাঠামোতে (হার্ডওয়্যার কিংবা সফটওয়্যার) অরক্ষিত অবস্থার কারণে অধিকাংশ হুমকির ঘটনা ঘটে। নিরাপত্তা হুমকির কারণে অনাকাঙ্ক্ষিত যে সকল ঘটনা ঘটিতে পারে তাহা হইলঃ

- ক. অননুমোদিত অনুপ্রবেশ
- খ. তথ্য প্রকাশ
- গ. আইনগত দুর্বলতার কারণে হুমকি
- ঘ. অন্তর্ঘাতী কাজ
- ঙ. নিরাপত্তা সতর্কতার অপ্রতুলতা
- চ. দুর্বল নিরাপত্তা পলিসি
- ছ. প্রতারণা
- জ. অত্যাধিক কাজের চাপ

- ঝ. সেবা গ্রহণে প্রতিবন্ধকতার উপস্থিতি (Denial of Service)
- ঞ. ঠকানো (Spoofing)
- ট. সর্বক্ষণ পরিলক্ষিত হুমকি (Advanced persistent threat)
- ঠ. ত্রুটিযুক্ত এপ্লিকেশন (Application with bugs)
- ড. আড়িপাতা ইত্যাদি।
- ঢ. পরিচিতি আত্মসাত (Identity Theft)
- ণ. ডিএনএস নিরাপত্তা হুমকি (DNS Security Threat)

(গ) অরক্ষিত অবস্থা

অরক্ষিত অবস্থা হইলে ত্রুটি বা দুর্বলতা যাহা কোনো সংস্থার সম্পদ বা সামর্থের সহিত সম্পৃক্ত। ইহা এক বা একাধিক কারণে সৃষ্ট হুমকির দ্বারা সম্পদের ক্ষতি করিতে পারে এমন অবস্থা। সুতরাং যে অরক্ষিত অবস্থা কোনো সম্পদের ক্ষতির হুমকি সৃষ্টি করিতে পারে না তাহা নিরাপত্তা ঝুঁকি হিসাবে গণ্য হইবে না। সাধারণত নিম্নলিখিত কারণে অরক্ষিত অবস্থা লক্ষ্য করা যায় :

- ক. ত্রুটিপূর্ণ পদ্ধতি
- খ. স্বল্প দক্ষ কর্মচারী,
- গ. ত্রুটিযুক্তভাবে স্থাপিত বা ত্রুটিযুক্ত প্রযুক্তি।

(ঘ) অরক্ষিত অবস্থাকে কাজে লাগাইবার জন্য একটি হুমকিকে অরক্ষিত অবস্থার যুগোপ গ্রহণের মত পরিস্থিতি থাকিতে হইবে। তথ্য সংশ্লিষ্ট নিরাপত্তার জন্য “জানিবার লক্ষ্যে প্রয়োজন” (Need to Know) নীতি অনুসরণ করিয়া জনবল ও প্রযুক্তি উভয় ক্ষেত্রে প্রয়োগ করিতে হইবে। সংস্থার জন্য ইহা গুরুত্বপূর্ণ হইবে যে অরক্ষিত অবস্থা সম্পর্ক জানা এবং যথাযথ ব্যবস্থা গ্রহণ করা। সম্ভবত অধিকাংশ অরক্ষিত অবস্থা হইল “সোশাল ইঞ্জিনিয়ারিং”-এর প্রতি কর্মচারীদের সংবেদনশীলতা। সকল কর্মচারীর জন্য নিরাপত্তা সচেতনতা একটি গুরুত্বপূর্ণ রক্ষাকবচ। সংশ্লিষ্ট সম্পদের আলোকে অরক্ষিত অবস্থাকে নিম্নলিখিতভাবে শ্রেণীবিন্যাস করা যায় :

- ক. প্রাতিষ্ঠানিক,
- খ. কর্মচারী সংশ্লিষ্ট,
- গ. পরিবেশগত,
- ঘ. হার্ডওয়্যার, সফটওয়্যার ও নেটওয়ার্ক সংক্রান্ত,
- ঙ. স্পেস সংক্রান্ত।

(৩) ঝুঁকি, হুমকি ও অরক্ষিত অবস্থা সনাক্তকরণ

কোনো সংস্থার তথ্য সম্পদসমূহকে অরক্ষিত অবস্থার কারণে উদ্ভূত হুমকির জন্য সৃষ্ট ঝুঁকি (যাহা তথ্য সম্পদ হারানো বা নষ্টের কারণ হইতে পারে) হইতে রক্ষার জন্য তথ্য নিরাপত্তা পলিসি প্রয়োজন। প্রায়শই লক্ষ্য করা যায় যে, বেশিরভাগ সংস্থাই ঝুঁকি, হুমকি ও অরক্ষিত অবস্থার সংজ্ঞাকে একত্রিত

করিয়া ফেলে। ঝুঁকি, হুমকি ও অরক্ষিত অবস্থা একই ধরনের অর্থ বহন করে এমন পরিভাষা নহে। এই তিনটি বিষয় পরিস্কারভাবে বুঝিবার সুবিধার্থে তথ্য সম্পদ, ঝুঁকি, হুমকি ও অরক্ষিত অবস্থায় তুলনামূলক সংজ্ঞাসমূহ নিম্নে উপস্থাপন করা হইলঃ

তথ্য সম্পদ	হুমকি	অরক্ষিত অবস্থা	ঝুঁকি
তথ্য সম্পদ এমন কিছু যাহা সংস্থা রক্ষা করিবার চেষ্টা করে।	যাহা হইতে কোনো সংস্থা তাহার তথ্য সম্পদ রক্ষা করিবার চেষ্টা করিয়া থাকে, তাহাই হুমকি।	কোনো সংস্থার সংরক্ষণ ব্যবস্থার মধ্যে যে দুর্বলতা বা ঘাটতি থাকে তাহারই অরক্ষিত অবস্থা।	অরক্ষিত অবস্থাজনিত হুমকির ফলে তথ্য সম্পদের যে ক্ষতি ঘটয়া থাকে অথবা বিনষ্ট হইবার সম্ভাবনা থাকে, তাহাই ঝুঁকি

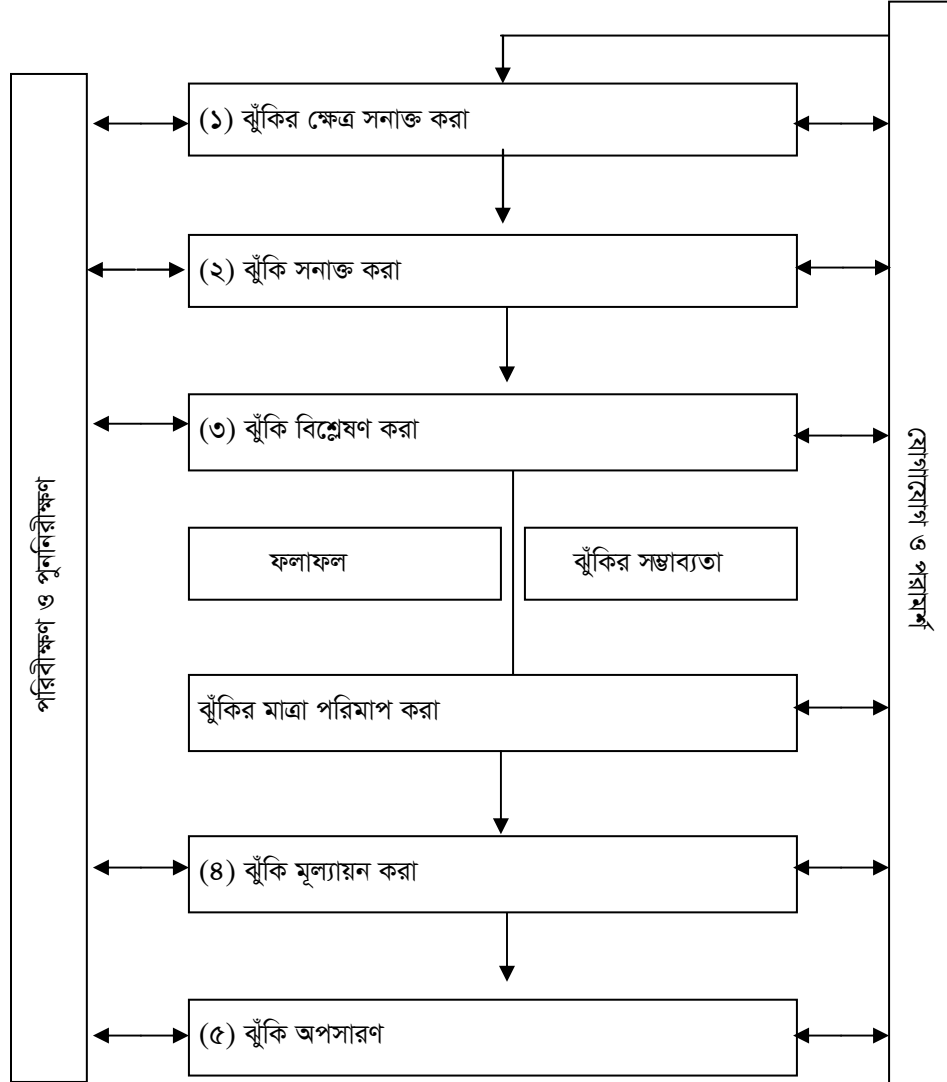
প্রতিটি সংস্থার জন্য তাহাদের স্ব স্ব তথ্য ব্যবস্থার ঝুঁকি, হুমকি ও অরক্ষিত অবস্থা সনাক্ত করিয়া সেই অনুযায়ী নিরাপত্তা নিয়ন্ত্রণ প্রয়োগ করা খুবই গুরুত্বপূর্ণ। তথ্যের শ্রেণিকরণ ও তথ্যের অবস্থা সংস্থার ঝুঁকি পরিমাপকরণ এবং নিরাপত্তা নিয়ন্ত্রণ প্রয়োগের কাজ সহজতর করিবে। ঝুঁকির মাত্রার তীব্রতা অনুযায়ী কোন সংস্থা তাহার সনাক্তকৃত সকল ঝুঁকির পরিমাপ নির্ধারণ করিবে। এই পরিমাপ নির্ধারণী বিষয়কে সংখ্যা ভিত্তিক স্কেলের মাধ্যমে সংজ্ঞায়িত করিতে হইবে এবং '০' হইতে '১০' পর্যন্ত মান ব্যবহার করা যাইতে পারে, যেখানে '০' সর্বনিম্ন মান এবং '১০' সর্বোচ্চ মান।

(৪) ঝুঁকি ব্যবস্থাপনা

ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার উদ্দেশ্য হইল হুমকি ও অরক্ষিত অবস্থা চিহ্নিত করিয়া তথ্য সম্পদের সংরক্ষণ নিশ্চিত করিবার জন্য প্রয়োজনীয় সুপারিশ প্রদান করা। ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া অভ্যন্তরীণ ও বহিঃ সম্পদের মাধ্যমে সম্পন্ন করা যাইতে পারে। সংস্থাকে ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া শুরু করিবার পূর্বে যেসকল বিষয় বিবেচনায় রাখিতে হইবে তাহা হইল :

- ক. নেটওয়ার্ক ও সফটওয়্যার ডিজাইন ও উন্নয়ন;
- খ. পরিবর্তন ব্যবস্থাপনা;
- গ. ভৌত নিরাপত্তা, প্রবেশাধিকার নিয়ন্ত্রণ;
- ঘ. বাহিরের অরক্ষিত অবস্থা বা অভ্যন্তরীণ অরক্ষিত অবস্থা;
- ঙ. সংরক্ষণ ও ব্যাকআপ কৌশল, পূর্ব অবস্থায় ফিরাইয়া আনার ব্যবস্থা ও পরীক্ষাকরণ;
- চ. অনির্ধারিত ঘটনার পরিকল্পনা/পরীক্ষা (দুর্যোগ পরবর্তী তথ্য পুনরুদ্ধার/কার্যক্রমের ধারাবাহিকতা);
- ছ. তথ্য প্রেরণ,
- জ. অপ্রয়োজনীয় তথ্য সম্পদ অপসারণ,
- ঝ. কর্মীদের দক্ষতা,
- ঞ. ইন্সিডেন্ট ব্যবস্থাপনার ইতিহাস,
- ট. সিস্টেম অডিটকরণ ইত্যাদি।

(৫) কোনো সংস্থার তথ্য নিরাপত্তা পলিসি প্রণয়নের জন্য তাহার ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া অবশ্যই নিরূপণ করিতে হইবে। ঝুঁকি ব্যবস্থাপনার ক্ষেত্রে ইউরোপীয় ইউনিয়ন ভিত্তিক CORAS প্রকল্প কর্তৃক এএস/এনজেডএস ৪৩৬০:২০০৪ এবং আইএসও/আইইসি ৩১০০০:২০০৯ মডেলের উপর ভিত্তি করিয়া ভালো ও গ্রহণযোগ্য মডেল প্রণয়ন করা হইয়াছে। বাংলাদেশের যে কোন সংস্থা এই মডেলটি গ্রহণ করিতে পারে অথবা তারা নিজস্ব কোন মডেল তৈরি করিতে পারে।



চিত্র-১ ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া

চিত্রে ঝুঁকি ব্যবস্থাপনা প্রক্রিয়া চক্রে ৫ (পাঁচ) টি ধাপ উল্লেখ করা হইয়াছে। ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার প্রতিটি ধাপের কার্যকারিতা ও উন্নয়নের জন্য উল্লম্বভাবে উপস্থাপিত কলামে পরিবীক্ষণ ও পুননিরীক্ষণ এবং যোগাযোগ ও পরামর্শ প্রয়োজনীয়। ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার ধাপগুলি হইল :

(৬) ঝুঁকির ক্ষেত্র সনাক্তকরণ

প্রসংগ সাব্যস্ত করিবার উদ্দেশ্য হইল বিশ্লেষণের উদ্দেশ্য ও তাহার পরিবেশকে চিহ্নিতকরণ। বাহ্যিক, অভ্যন্তরীণ ও ঝুঁকি ব্যবস্থাপনা বিষয়ক ক্ষেত্র হইতে পারে যাহাতে প্রক্রিয়ার অবশিষ্ট অংশ সম্পন্ন হইবে। যে সকল বৈশিষ্ট্যের ঝুঁকি মূল্যায়িত হইবে তাহাদের সাব্যস্ত করিতে হইবে এবং বিশ্লেষণের কাঠামো সুস্পষ্টভাবে ব্যাখ্যা করিতে হইবে।

(৭) ঝুঁকি চিহ্নিত করা

এই ধাপে সংস্থাকে কোথায়, কখন, কেন ও কিভাবে কোন ইন্সিডেন্ট ঘটিতে পারে তাহা চিহ্নিত করিতে হইবে, অর্থাৎ হুমকি সনাক্তকরণ যাহা বা যে অবস্থা ইন্সিডেন্ট ঘটাইতে পারে তাহা চিহ্নিতকরণই অরক্ষিত অবস্থা সনাক্তকরণ। ইহা করিবার সময় তথ্যসম্পদের শ্রেণিকরণ সম্পন্ন করার বিষয়ে সুপারিশ প্রদান করা হইল।

(৮) ঝুঁকি বিশ্লেষণ করা

এই ধাপে, সংস্থা তাহার ঝুঁকি পরিমাপ করিবে। এইখানে সংস্থা তাহার বিরাজমান নিয়ন্ত্রণকে চিহ্নিত ও মূল্যায়ন করিবে। তারপর সংস্থাটি পরিণতি ও সম্ভাব্যতা নির্ধারণ করিবে এবং তাহাই হইল উহার ঝুঁকির মাত্রা। এই বিশ্লেষণে সম্ভাব্য ফলাফল এবং কিভাবে এই সকল ঘটিতে পারে তাহা বিবেচনা করিতে হইবে।

(৯) ঝুঁকি মূল্যায়ন করা

ঝুঁকিকে কিভাবে বিবেচনা করিতে হইবে সেই সম্বন্ধে সিদ্ধান্ত গ্রহণ করিবার ক্ষেত্রে এইটি একটি খুবই গুরুত্বপূর্ণ ধাপ। এই ধাপে, ঝুঁকি বিশ্লেষণের ফলাফলের উপর ভিত্তি করিয়া সংস্থা ঝুঁকিসমূহকে বিভাবে বিবেচনা করিবে সেই বিষয়ে সিদ্ধান্ত গ্রহণ করিবার জন্য ঝুঁকির ফলাফল ও তাহার সহিত সংশ্লিষ্ট ঝুঁকির মানসমূহের একটি মানচিত্র তৈরি করিবে। সেই ক্ষেত্রে কিছু ঝুঁকি বিবেচনায় আসিবে যাহার মধ্যে কোনো ব্যবস্থা গ্রহণ করিবার প্রয়োজন নাই। এইখানে সংস্থা ঝুঁকি নিরসনের ক্ষেত্রে অগ্রাধিকার তালিকা প্রস্তুত করিবে।

(১০) ঝুঁকি অপসারণ করা

পূর্ববর্তী ধাপসমূহ হইতে প্রাপ্ত ফলাফল অনুযায়ী সংস্থা কার্যকর পরিকল্পনা ও ঝুঁকি নিরসনের পদ্ধতি প্রণয়ন করিতে পারিবে। সর্বোচ্চ দক্ষতা কাজে লাগাইয়া সর্বনিম্ন ব্যয়ে বাস্তবায়নযোগ্য। যোগ্য পরিকল্পনা প্রস্তুত করিবার জন্য সর্বদাই সুপারিশ করা হইয়া থাকে। ঝুঁকি নিরসন কাজের মধ্যে ঝুঁকি এড়াইয়া যাওয়া, ঝুঁকি স্থানান্তর করা, কিছু ঝুঁকি রাখিয়া দেওয়া, সম্ভাব্যতার পরিবর্তন ও ঝুঁকির পরিণতি প্রভৃতি বিষয় অন্তর্ভুক্ত।

(১১) ঝুঁকি ব্যবস্থাপনা আদর্শ কাঠামো (Template)

সংস্থাকে ঝুঁকি ব্যবস্থাপনা প্রক্রিয়ার জন্য অবশ্যই একটি মানদণ্ড তৈরি করিতে হইবে এবং এই ঝুঁকি বিশ্লেষণে কোনো একটি সংস্থার সারা জীবনব্যাপী সময়ের মধ্যে অবশ্যই একটি নির্দিষ্ট সময়ভিত্তিক প্রক্রিয়া থাকিতে হইতে হইবে। ঝুঁকি ব্যবস্থাপনার গ্রহণযোগ্য কাঠামো হইল ক্ষেত্রসংবলিত একটি সাধারণ ফরম যাহাকে কোনো সংস্থা সময়ে সময়ে ঝুঁকি বিশ্লেষণ সম্পন্ন করিবার মাধ্যমে পূরণ করিবে। এই গাইডলাইনে একটি নমুনা কাঠামো উপস্থাপন করা হইল :

তথ্য সম্পদ		হুমকি বিশ্লেষণ		অরক্ষিত অবস্থা বিশ্লেষণ		ঝুঁকি বিশ্লেষণ		উত্তরণের জন্য করণীয় কর্মপরিকল্পনা	মন্তব্য
বিস্তারিত	শ্রেণি ও অবস্থা	নাম	বিস্তারিত	নাম	বিস্তারিত	বিস্তারিত	মাত্রা		

(১২) অনুচ্ছেদ অনুযায়ী করণীয়

এই অনুচ্ছেদে তথ্য নিরাপত্তা কৌশলের ধাপ সম্পর্কিত কার্যাবলীর বর্ণনা করা হইয়াছে যাহাতে অনুচ্ছেদ ৮.১, বিশেষত পর্যায় ২: অনুধাবন, পর্যায় ৪: বাস্তবায়ন এবং পর্যায় ৬: মূল্যায়ন ও পরিবীক্ষণ এর ব্যাখ্যা রহিয়াছে। ঝুঁকি ব্যবস্থাপনা পলিসি অপেক্ষা কার্যক্রমের উপর বেশী নির্ভরশীল। সংস্থা যখন তাহার নিরাপত্তা পলিসি ডকুমেন্ট তৈরি করিবে তখন উহাতে কর্মপদ্ধতি বা ঝুঁকি পরিমাপের ব্যাখ্যা ও উহাকে গ্রহণ করিবার কারণ অন্তর্ভুক্ত থাকিতে হইবে। নিম্নলিখিত বিষয়গুলি ঝুঁকি ব্যবস্থাপনার কর্মপদ্ধতি বা সমন্বিত ঝুঁকি ব্যবস্থাপনা মডেলে অন্তর্ভুক্ত করিবার জন্য সুপারিশ করা হইয়া থাকে:—

- ক. ঝুঁকি পরিমাপ কতবার করিতে হইতে পারে তাহা নির্ধারণ,
- খ. তথ্য সমাগম,
- গ. হুমকি ও অরক্ষিত অবস্থা বিশ্লেষণ,
- ঘ. ঝুঁকি সনাক্তকরণ
- ঙ. ঝুঁকি বিশ্লেষণ ও মূল্যায়ন,
- চ. ঝুঁকি নিরসন,
- ছ. পরিবীক্ষণ ও পরীক্ষা, নিরীক্ষা
- জ. ঝুঁকি পরিমাপ মানদণ্ড।

ঝুঁকি ব্যবস্থাপনা হইল তথ্য সম্পদ রক্ষা করিবার জন্য একটি খুবই গুরুত্বপূর্ণ অংশ। এই অনুচ্ছেদে, ঝুঁকি ব্যবস্থাপনা সম্পর্কিত বিভিন্ন বিষয়ের সংক্ষিপ্ত ব্যাখ্যা থাকিবে। আরও বিস্তারিত তথ্যের জন্য সংস্থাকে আইএসও (আদর্শ মানদণ্ডের জন্য আন্তর্জাতিক সংস্থা/আইইসি (আন্তর্জাতিক ইলেক্ট্রোটেকনিক্যাল কমিশন) ২৭০০০ আইএও আইইসি ৩১০০০, এএস (অস্ট্রেলীয় মানদণ্ড/এনজিএস) ৪৩৬০:২০০৪-এর অনুমোদিত হইতে পারে এবং ইউরোপীয় CORAS কর্তৃক অনুমোদিত ঝুঁকি বিশ্লেষণের জন্য নিরাপত্তার সঙ্কটপূর্ণ সিস্টেমের একটি প্লাটফর্ম থাকিতে পারে।

১০. তথ্য রক্ষায় নিরাপত্তা নিয়ন্ত্রণ

(১) নিরাপত্তা নিয়ন্ত্রণ হইল এমন রক্ষাকবচ যাহার মাধ্যমে ঝুঁকি এড়ানো বা হ্রাস করা হয়। নিরাপত্তা নিয়ন্ত্রণের রূপরেখা পর্যালোচনা বা ডিজাইনে সাহায্য করিবার জন্য নিয়ন্ত্রণের একটি শ্রেণিকরণ করা যাইতে পারে। নিরাপত্তা নিয়ন্ত্রণের সময় অনুসারে ভাগ করা যাইতে পারে; যথা:—

- ক. ঘটনা ঘটিবার আগে, প্রতিরোধমূলক নিয়ন্ত্রণ;
- খ. ঘটনা ঘটিবার সময়, সনাক্তকরণ/চিহ্নিতকরণ নিয়ন্ত্রণ;
- গ. ঘটনা ঘটিবার পর, সংশোধনমূলক নিয়ন্ত্রণ;

(২) নিরাপত্তা নিয়ন্ত্রণসমূহকে উহাদের প্রকৃতি অনুযায়ী বিভিন্ন ক্যাটাগরিতে বিভক্ত করা যাইতে পারে, উদাহরণস্বরূপ:—

- ক. ভৌত নিয়ন্ত্রণ;
- খ. পদ্ধতিগত নিয়ন্ত্রণ;
- গ. কারিগরি নিয়ন্ত্রণ;
- ঘ. আইন ও মান অনুসরণমূলক নিয়ন্ত্রণ।

(৩) পৃথিবীতে তথ্য নিরাপত্তা নিয়ন্ত্রণ বা গভর্নেন্সের ক্ষেত্রে অনেক উত্তম দৃষ্টান্ত রহিয়াছে, তাহাদের মধ্যে উল্লেখযোগ্য হইল:—

- ক. আইএসও/আইইসি ২৭০০১, আইএসও/আইইসি ২৭০০২
- খ. সিওবিআইটি ৪.১ বা পরবর্তী সংস্করণ
- গ. আইটিআইএল ভি৩ বা পরবর্তী সংস্করণ

(৪) নিরাপত্তা নিয়ন্ত্রণের উল্লিখিত উত্তম দৃষ্টান্তগুলি বৃহত্তর আঙ্গিকে অনুসরণযোগ্য এবং সংস্থাকে ব্যয় সাশ্রয়ী উপায়ে তাহাদের প্রয়োজন অনুযায়ী অবশ্যই সেইসব মানদণ্ড অথবা উত্তম দৃষ্টান্তগুলি পুনর্গঠন করিতে হইবে। নিরাপত্তা নিয়ন্ত্রণ গ্রহণকালে তথ্যসম্পদের শ্রেণিবিভাগ বিবেচনা করিতে হইবে। যে তথ্য সম্পদ গোপনীয় নহে তাহার নিরাপত্তা নিয়ন্ত্রণ গ্রহণের ক্ষেত্রে খুব বেশি কঠোর নিয়ন্ত্রণের প্রয়োজনীয়তা নাই। আইএসও/আইইসি ২৭০০২ হইতে গৃহীত কতগুলি নিরাপত্তা নিয়ন্ত্রণ উদাহরণ নিম্নে উল্লেখ করা হইল:—

- ক. কর্মীদের নিরাপত্তা,
- খ. যন্ত্রপাতির নিয়ন্ত্রণ,
- গ. প্রবেশাধিকার নিয়ন্ত্রণ,
- ঘ. ভৌত ও পরিবেশগত নিরাপত্তা ব্যবস্থা,
- ঙ. কর্মসম্পাদন পদ্ধতি ও দায়িত্বশীলতা,

- চ. তৃতীয়পক্ষের সেবা প্রদান ব্যবস্থাপনা,
- ছ. সিস্টেম পরিকল্পনা ও গ্রহণযোগ্যতা,
- জ. এ্যাপ্লিকেশন নিরাপত্তা,
- ঝ. ক্ষতিকারক কোডের বিরুদ্ধে প্রতিরোধ ব্যবস্থা,
- ঞ. তথ্য ব্যাক-আপ,
- ট. নেটওয়ার্ক নিরাপত্তা-ব্যবস্থাপনা,
- ঠ. অপসারণযোগ্য যন্ত্রাদির যথাযথ ব্যবহার,
- ড. তথ্য বিনিময়/প্রেরণ
- ঢ. তথ্য নিষ্পত্তি,
- ণ. তথ্য ব্যবস্থার নিরাপত্তা,
- ত. ক্রিপ্টোগ্রাফিক নিয়ন্ত্রণ,
- থ. সঠিক প্রক্রিয়াকরণ,
- দ. সিস্টেম ফাইল নিরাপত্তা,
- ধ. পরিবীক্ষণ ইত্যাদি।

এইসব নিয়ন্ত্রণ ব্যবস্থা সম্পর্কে আরও জানিতে চাইলে আইএসও/আইইসি ২৭০০২ পাঠ করা যাইতে পারে এবং সংস্থাকে অবশ্যই তাহার তথ্য সংরক্ষণের জন্য কোথায় ও কোন ধরনের নিয়ন্ত্রণ ব্যবস্থার প্রয়োজন হইবে সে বিষয়ে সিদ্ধান্ত গ্রহণ করিতে হইবে।

(৫) তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ এ উল্লিখিত জাতীয় পিকেআই ইতোমধ্যে চালু হইয়াছে এবং ইহা তথ্য ও যোগাযোগ প্রযুক্তি মন্ত্রণালয়ের অধীন ইলেক্ট্রনিক স্বাক্ষর সার্টিফায়িং অথরিটির নিয়ন্ত্রণাধীন রহিয়াছে। সংস্থাকে অবশ্যই ডিজিটাল স্বাক্ষর সার্টিফিকেট ব্যবস্থা রাখিতে হইবে এবং পিকেআই-সক্ষম এপ্লিকেশনের মাধ্যমে উহাদের ক্রিপ্টোগ্রাফিক নিয়ন্ত্রণ নিশ্চিত করিতে হইবে। ডিজিটাল স্বাক্ষর সার্টিফিকেট তথ্য নিরাপত্তার চারটি লক্ষ্য নিশ্চিত করে, সেইগুলি হইল:

- ক. সঠিকতা (তথ্য বিনিময়ে সম্পৃক্ত তথ্য ও পক্ষসমূহের সঠিকতা)
- খ. গোপনীয়তা (এনক্রিপশন প্রযুক্তি ব্যবহারের মাধ্যমে তথ্যের গোপনীয়তা নিশ্চিতকরণ)
- গ. তথ্য সম্পদের শুদ্ধতা (তথ্য ব্যবহারকারীদের তথ্যের পরিবর্তন হয় নাই এমন নিশ্চয়তা প্রদান)
- ঘ. অনস্বীকৃতি (তথ্য উদ্ভাবনকারী বা স্বাক্ষরকারী আইনগতভাবে এই মর্মে চ্যালেঞ্জ করিতে পারিবেন না যে, তিনি বা তাহারা তথ্যে স্বাক্ষর বা তথ্য উদ্ভাবন করেন নাই)।

১১। আইনগত ও প্রায়োগিক বিষয়

(১) সংস্থা যখন উহার পলিসি প্রণয়ন করিবে, তখন অবশ্যই আইনগত ও প্রায়োগিক বিষয়সমূহ যাহা পলিসি দ্বারা প্রভাবিত হইতে পারে, তাহার প্রতি সংস্থাকে সচেতন থাকিতে হইবে। আইন বা নিয়মের বাধ্যবাধকতার ক্ষেত্রে যে কোনো ব্যত্যয় এড়াইতে এবং অন্যান্য পলিসির সহিত বিরোধ এড়াইতে আইন ও প্রায়োগিক সংক্রান্ত বাহ্যিক ও অভ্যন্তরীণ উভয় বিষয় বিবেচনা করা খুবই গুরুত্বপূর্ণ। পলিসি প্রণয়নকালে সংস্থা কর্তৃক বিবেচ্য আইন ও পলিসির একটি তালিকা দেওয়া হইল:

- ক. তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (সংশোধিত ২০০৯)
- খ. তথ্য ও যোগাযোগ প্রযুক্তি পলিসি, ২০০৯
- গ. তথ্য অধিকার আইন, ২০০৯
- ঘ. মেধাসত্ত্ব অধিকার, ১৯১১
- ঙ. কপিরাইট অ্যাক্ট, ২০০০ (২০০৫ এ সংশোধিত)
- চ. ক্রিপটোগ্রাফিক নিয়ন্ত্রণের জন্য PKI সম্পর্কিত বিধি/২০১০
- ছ. জাতীয় আরকাইভ আইন, ১৯৮৩
- জ. সাইবার নিরাপত্তা সম্বন্ধীয় আইন/গাইডলাইন/পলিসি;
- ঝ. জাতিসংঘ কনভেনশন/ইন্টারনেট বা সাইবার নিরাপত্তা সম্বন্ধীয় আইন।

(২) ইন্টারনেট বা সাইবার নিরাপত্তা বিষয়ে সরকারের নিয়ন্ত্রণাধীন সংস্থাকে এমন পলিসি প্রণয়ন করিতে হইবে যাহা অবশ্যই জাতীয় আইন-কানুন, নীতি ও গাইডলাইনসমূহের সাথে সামঞ্জস্যপূর্ণ থাকে। তথ্য নিরাপত্তা নীতির বিবরণীতে কোন সংস্থাকে অবশ্যই দেশের প্রচলিত আইন, বিধি এবং অপরাপর নীতি/গাইডলাইন/স্ট্যান্ডার্ড উল্লেখ করিতে হইবে। বিক্রেতা প্রতিষ্ঠান অথবা তথ্য ও যোগাযোগ প্রযুক্তি সম্পর্কিত অন্য যেকোনো সরকারি সংস্থার (হার্ডওয়্যার, সফটওয়্যার, নেটওয়ার্ক বা অন্য কোনো তথ্য পদ্ধতি) সেবা গ্রহণ করিবার পূর্বে সংস্থাকে অবশ্যই Service Level Agreement বিবেচনা করিতে হইবে।

১২। মানদণ্ড ও গাইডলাইন

কোন সংস্থার তথ্য নিরাপত্তা পলিসি বাস্তবায়নের ধাপসমূহ নির্ধারণ করে না এবং কোন পলিসির সফল বাস্তবায়নের জন্য সংস্থা কর্তৃক অনুসৃত কোন মানদণ্ডের ব্যাখ্যা প্রদান করে না। পলিসি অনুসরণের সময়ই মানদণ্ড ও গাইডলাইন কাজে আসে। কিন্তু কোন সংস্থার তথ্য সম্পদ সুরক্ষার প্রতিটি পর্যায়ে আবশ্যিকভাবে সংস্থা কর্তৃক মানদণ্ড ও গাইডলাইন নির্ধারণের বিষয়ে পলিসি ডকুমেন্টে কিছু নির্দেশনা থাকা প্রয়োজন। পলিসি ডকুমেন্টে প্রয়োজনীয়তার নিরিখে কিছু নির্দেশনা ও মানদণ্ড অন্তর্ভুক্ত হইতে পারে।

১৩। তথ্য ব্যবস্থা নিরীক্ষা ও প্রত্যয়ন

(১) যে সকল সংস্থা গুরুত্বপূর্ণ তথ্য ব্যবস্থা অবকাঠামো পরিচালনা করিয়া থাকে তাহাদের অবশ্যই সময়ে সময়ে তথ্য অডিট করাইতে হইবে। এইক্ষেত্রে অডিটর সংস্থার ভিতরের, বাইরের, অথবা উভয় ধরনের হইতে পারিবে। কোন সংস্থার পরিচালনা পদ্ধতির যে কোন ধরনের বিপর্যয় ন্যূনতম পর্যায়ে রাখাসহ কর্মতৎপরতার উন্নয়নে তথ্য ব্যবস্থার অডিট অত্যন্ত গুরুত্বপূর্ণ। তথ্য ব্যবস্থার অডিট পরিবীক্ষণ ও পুনর্মূল্যায়নের পর্যায় ৬ এর অংশ।

(২) প্রত্যয়ন হইল কোন তৃতীয় পক্ষ কর্তৃক কোন সংস্থার তথ্য ব্যবস্থার অবকাঠামো এবং তথ্য নিরাপত্তা ব্যবস্থাপনা পদ্ধতি যাচাইয়ের ভিত্তিতে এক ধরনের বাহ্যিক মূল্যায়ন। মূল্যায়নের নির্ণায়কসমূহ সর্বদাই মানদণ্ড কর্তৃপক্ষ কর্তৃক নিয়ন্ত্রিত হইয়া থাকে। কোন সংস্থার বিষয়ে উক্ত সংস্থার অভ্যন্তরীণ ও বহিরাগত স্টেহোল্ডারদের নিকট প্রত্যয়নের মাধ্যমে নিশ্চয়তা প্রদান করা হইয়া থাকে। কোন সংস্থা ISO/IEC 27001 অনুযায়ী প্রত্যয়ন প্রত্যাশা করার পূর্বেই এর মূল্যায়নের নির্ণায়কসমূহ জানিয়া নিতে হইবে। কার্যবিধিতে প্রদত্ত ক্ষমতাবলে বাংলাদেশ কম্পিউটার কাউন্সিল তথ্য নিরাপত্তা ব্যবস্থাপনা পদ্ধতি (আই এস এম এস) বাস্তবায়নকারী সংস্থাসমূহের প্রত্যয়ন কার্যক্রম আরম্ভ করিতে পারে। মান বিষয়ক প্রত্যয়ন সংস্থাসমূহের কর্ম পরিবেশ ও কর্মক্ষমতা উন্নয়নে সহায়তা করে।

১৪। ইন্সিডেন্ট ব্যবস্থাপনা

(১) তথ্য নিরাপত্তা বিঘ্নকারী ঘটনা হইল কোন একক অথবা একগুচ্ছ অনাকাঙ্ক্ষিত বা অপ্রত্যাশিত তথ্য নিরাপত্তা বিষয়ক ইভেন্ট যাহার কারণে চাপের মুখে প্রতিষ্ঠানকে তাহার কর্মকাণ্ড সংকুচিত করিবার হুমকির যথার্থ সম্ভাবনা থাকে। তথ্য নিরাপত্তার ক্ষেত্রে কোন ইন্সিডেন্ট ঘটিবার পূর্বেই ইন্সিডেন্ট ব্যবস্থাপনার পরিকল্পনার বিষয়ে বিবেচনা করাটা খুবই গুরুত্বপূর্ণ। কাহারো পক্ষে কোন কর্মকাণ্ড সম্পাদনের ক্ষেত্রে কখন ও কি ধরনের বিঘ্ন সৃষ্টিকারী ইন্সিডেন্ট ঘটিবে তাহা পূর্বেই সঠিকভাবে জানা সম্ভব নয়। তথ্য নিরাপত্তা বিষয়ক ইন্সিডেন্ট যে কোন সময় ঘটিতে পারে। কোন ইন্সিডেন্ট মোকাবেলা করিবার জন্য শক্তিশালী ও কার্যকর প্রক্রিয়া প্রতিষ্ঠা করা খুবই জরুরী।

(২) ইন্সিডেন্ট প্রাকৃতিক অথবা মনুষ্য-সৃষ্ট হইতে পারে। উভয় ক্ষেত্রে কার্যকর ইন্সিডেন্ট ব্যবস্থাপনা নির্ভর করিবে কত সুচারুভাবে ব্যবস্থাপনাটি কোন ইন্সিডেন্ট মোকাবেলা করিতে পারে তাহার উপর। প্রাকৃতিক ঘটনার ক্ষেত্রে, উদাহরণস্বরূপ বন্যা বা অগ্নিকাণ্ড বা ভূমিকম্প অথবা যে কোন ধরনের প্রাকৃতিক দুর্যোগের সময়ে কর্মকাণ্ডের ধারাবাহিকতা রক্ষার্থে তথ্য ব্যবস্থার পুনরুদ্ধারের কার্যক্রম শুরু করিতে হয়।

(৩) মানুষ দ্বারা সৃষ্ট আক্রমণ হিসাবেও ইন্সিডেন্ট ঘটিয়া থাকে। মনুষ্য-সৃষ্ট ঘটনার ক্ষেত্রে তথ্য নিরাপত্তা ইন্সিডেন্ট যথাসম্ভব সম্ভব যথাযথ ব্যবস্থাপনা চ্যানেলের মাধ্যমে রিপোর্ট করিতে হয়। অভ্যন্তরীণ অথবা বাহিরের বিশেষজ্ঞ অথবা তথ্য নিরাপত্তা ইন্সিডেন্ট পর্যবেক্ষক দলকে ঘটনা ঘটিবার পরপরই তদন্তপূর্বক যথাযথ রিপোর্ট প্রদান করিতে হইবে। ইহাও জরুরী যে, অভ্যন্তরীণ সকল কর্মচারীকে জানিতে হইবে যে, কোন ঘটনা ঘটিবার পর প্রমাণসমূহ অপরিবর্তনীয় অবস্থায় রাখিতে হইবে। কোন ইন্সিডেন্টের সফল তদন্তের পর ইহার রেকর্ড রাখিতে হইবে যাহাতে ঝুঁকি ব্যবস্থাপনা পদ্ধতির উন্নয়ন ঘটানো যায়। তাহা ছাড়া ইন্সিডেন্টের মূল্যায়ন রিপোর্ট প্রয়োজনীয়তার নিরিখে যথাযথ কার্যক্রম গ্রহণের নিমিত্ত ব্যবস্থাপনা কর্তৃপক্ষকে জানাইতে হইবে।

(৪) তথ্য নিরাপত্তা পলিসি ডকুমেন্টে ইসিডেন্ট ব্যবস্থাপনা সম্বন্ধে অবশ্যই কিছু দিক নির্দেশনা থাকিতে হইবে। ইসিডেন্ট ব্যবস্থাপনা বিষয়ে যথাযথ ধারণার জন্য প্রতিটি সংস্থা আইএসও/আইইসি টি আর ১৮০৪৪:২০০৪ পাঠ করিতে পারে।

১৫। কার্যক্রমের ধারাবাহিকতা বিষয়ক পরিকল্পনা

(১) তথ্য ব্যবস্থাপনায় কোনো ত্রুটির জন্য অথবা কোনো বিপর্যয়ের কারণে দৈনন্দিন কার্যক্রম বিঘ্নিত হইলে উহাদের পুনরারম্ভ সময়মতো হওয়ার বিষয়টি নিশ্চিত করিবার জন্য কার্যক্রমের ধারাবাহিকতা রক্ষায় ব্যবস্থাপনা প্রক্রিয়া বাস্তবায়ন করিতে হইবে। দুর্বিপাকের ফলে (যাহা প্রাকৃতিক দুর্যোগ, দুর্ঘটনা, যান্ত্রিক বিফলতা ও ইচ্ছাকৃত কার্যাবলির ফলে উদ্ভূত হইয়া থাকে) সংস্থার উপর স্পষ্ট প্রভাব কমাইয়া রাখার এবং প্রতিরোধমূলক ও পুনরুদ্ধারমূলক সমন্বিত পদক্ষেপের মাধ্যমে তথ্য সম্পদের ক্ষতির পরিমাণ গ্রহণযোগ্য মাত্রায় রাখা খুবই গুরুত্বপূর্ণ। এই প্রক্রিয়ার মাধ্যমে গুরুত্বপূর্ণ দৈনন্দিন কার্যক্রমের প্রক্রিয়াগুলিকে সনাক্ত করা এবং কার্যক্রমের ধারাবাহিকতা সংশ্লিষ্ট তথ্য নিরাপত্তা ব্যবস্থাপনার প্রক্রিয়ার সাথে অন্যান্য বিষয়সমূহ যেমন-পরিচালনা, জনবল, সম্পদ, যানবাহন, ভবন সংক্রান্ত বিষয় সমন্বিত করা প্রয়োজন।

(২) তথ্য নিরাপত্তা বিষয়টি দৈনন্দিন কার্যক্রমের ধারাবাহিকতার প্রক্রিয়া ও সংস্থার অন্যান্য ব্যবস্থাপনা প্রক্রিয়াসমূহের একটি অপরিহার্য অংশ। দৈনন্দিন কার্যক্রমের ধারাবাহিকতা ব্যবস্থাপনা ঝুঁকি সনাক্তকরণ ও হ্রাসকরণকে অন্তর্ভুক্ত করে। সেই সাথে এই প্রক্রিয়াটি সাধারণ ঝুঁকি নির্ণয়, ঘটনাসমূহের ক্ষতিকর প্রভাব কমিয়ে রাখা এবং দৈনন্দিন কার্যক্রমের জন্য প্রয়োজনীয় তথ্য সহজলভ্য হওয়ার বিষয় নিশ্চিত করবে। দৈনন্দিন কার্যক্রমের ধারাবাহিকতা বিষয়ক পরিকল্পনার (আইএসও/আইইসি ২৭০০২ অনুযায়ী) বিভিন্ন ধাপ উল্লেখ করা হইল :

- ক. কার্যক্রমের ধারাবাহিকতা ব্যবস্থাপনা প্রক্রিয়ায় তথ্য নিরাপত্তা অন্তর্ভুক্তিকরণ;
- খ. কার্যক্রমের ধারাবাহিকতা ও ঝুঁকি নির্ণয়করণ;
- গ. তথ্য নিরাপত্তাসহ ধারাবাহিকতা পরিকল্পনার উন্নয়ন ও বাস্তবায়ন;
- ঘ. কার্যক্রমের ধারাবাহিকতা পরিকল্পনার নির্দেশাবলি;
- ঙ. কার্যক্রমের ধারাবাহিকতা পরিকল্পনা পরীক্ষাকরণ, ত্রুটি অপসারণ ও শুদ্ধিকরণ।

প্রত্যেকটি সংস্থাকে উহার একটি কার্যক্রমের ধারাবাহিকতা ব্যবস্থাপনা পরিকল্পনা প্রস্তুত করিবার জন্য ISO/IEC 27002 অনুসরণ করা এবং তথ্য নিরাপত্তা পলিসি ডকুমেন্টে ইহা ব্যবহারের সুস্পষ্ট দিকনির্দেশনা থাকিতে পারে।

১৬। পরিবীক্ষণ ও উন্নয়ন

(১) তথ্য নিরাপত্তা পলিসির উন্নয়নের জন্য ইহার পরিবীক্ষণ ও মূল্যায়ন করা একটি গুরুত্বপূর্ণ কাজ। তথ্য নিরাপত্তা কৌশলের বিভিন্ন ধাপ রহিয়াছে যাহা অনুচ্ছেদ-৮-এ বর্ণিত হইয়াছে। উল্লিখিত প্রত্যেকটি ধাপের সেবার মান উন্নয়নের জন্য প্রতিটি ধাপে পরিবীক্ষণ প্রয়োজন। পরিবীক্ষণ সম্বন্ধে এই অনুচ্ছেদে যাহা বলা হইতেছে তাহা ৮.১.৬ অনুচ্ছেদে বর্ণিত পরিবীক্ষণ হইতে আলাদা। পরিবীক্ষণ সম্পর্কে এখন যাহা বলা হইতেছে তাহা তথ্য নিরাপত্তা পলিসির কার্যকারিতার উপর পরিবীক্ষণ। এই পরিবীক্ষণের উদ্দেশ্য হইতেছে সংস্থা কর্তৃক কিভাবে পলিসি বাস্তবায়িত হইতেছে তাহা অনুধাবন করা

এবং বাস্তবায়নের ক্ষেত্রে কী কী প্রতিবন্ধকতা রহিয়াছে তাহা জানা। সেইসাথে তথ্য নিরাপত্তার বিষয়ে অথবা ব্যবস্থাপনার দৃষ্টিকোণ হইতে গুরুত্বপূর্ণ কোন পরিবর্তনের কারণে পলিসির পরিবর্তন বা পরিবর্ধন প্রয়োজন আছে কিনা, থাকিলে কী কী পরিবর্তন হইয়াছে এবং ফলশ্রুতিতে কী কী কার্যক্রম প্রয়োজন তাহা নির্ধারণ করা।

(২) পলিসি ডকুমেন্টে পরিবীক্ষণ বিষয়ক নির্দেশনা থাকিতে হইবে (যেমনঃ পরিবীক্ষণকারী কে হইবে, কতবার পরিবীক্ষণ করিতে হইবে, পরিবীক্ষণের ফলাফল কি, কাহার নিকট ইহা রিপোর্ট করিতে হইবে, পলিসির উন্নয়নের জন্য কোন স্টেকহোল্ডারদের মতামত বা পরামর্শ গ্রহণ করিতে হইবে প্রভৃতি)।

১৭। জাতীয় সাইবার নিরাপত্তা কৌশল

কোনো সংস্থার জন্য সাইবার নিরাপত্তা বিধানের লক্ষ্যে তথ্য নিরাপত্তা ঝুঁকি, নিরাপত্তা হুমকি ও অরক্ষিত অবস্থা সম্বন্ধে সতর্ক থাকা জরুরী। এই নির্দেশনাপত্র ছাড়াও একটি জাতীয় সাইবার নিরাপত্তা কৌশল প্রস্তুত করা প্রয়োজন রহিয়াছে। তদুপরি, ভবিষ্যতে সাইবার নিরাপত্তা ও তথ্য নিরাপত্তা বিষয়ক কর্মকাণ্ড পরিচালনা করিবার জন্য সরকার একটি পৃথক সংস্থা প্রতিষ্ঠা করিবে যাহা ‘বাংলাদেশ জাতীয় তথ্য নিরাপত্তা সংস্থা (বিএনআইএসএ)’ নামে অথবা উপযুক্ত অন্য কোনো নামে অভিহিত হইতে পারে।

১৮। পরিশিষ্ট ক: তথ্য নিরাপত্তা পলিসির গ্রহণযোগ্য কাঠামো

(১) তথ্য নিরাপত্তা পলিসি ডকুমেন্টে অবশ্যই ব্যবস্থাপনার প্রতিশ্রুতিসমূহ এবং তথ্য নিরাপত্তা ব্যবস্থাপনায় প্রতিষ্ঠানের গৃহীত উদ্যোগের বিষয় বিবৃত থাকিতে হইবে। পলিসি ডকুমেন্টে অবশ্যই নিম্নলিখিত বিষয় অন্তর্ভুক্ত থাকিবে:

(ক) তথ্য নিরাপত্তার সংজ্ঞা, উহার সার্বিক উদ্দেশ্য ও ক্ষেত্র এবং তথ্য বিনিময়ে একটি কার্যকর কৌশল হিসাবে তথ্য নিরাপত্তার গুরুত্ব।

(খ) প্রতিষ্ঠানের কার্যক্রম এবং উদ্দেশ্যের সহিত সঙ্গতিপূর্ণ তথ্য নিরাপত্তার উদ্দেশ্য ও মূলনীতি বাস্তবায়নে সহায়ক প্রতিষ্ঠানের এমন কার্যক্রমের বর্ণনা।

(গ) ঝুঁকি নির্ণয় ও ঝুঁকি ব্যবস্থাপনা সম্বলিত সুনির্দিষ্ট দালিলিক কাঠামো যাহাতে নিয়ন্ত্রণের উদ্দেশ্য এবং নিয়ন্ত্রণসমূহের বর্ণনা থাকিবে।

(ঘ) নিরাপত্তা পলিসি, মূলনীতি, মানদণ্ড ও প্রতিষ্ঠানের নিজস্ব প্রায়োগিক ক্ষেত্র বিবেচনায় অনুসরণীয় এমন বিষয়ের ব্যাখ্যা যাহার মধ্যে নিম্নোক্ত বিষয়সমূহ অন্তর্ভুক্ত থাকিবেঃ

- i) আইন, প্রশাসনিক নিয়ন্ত্রণ ও চুক্তির কারণে অনুসরণীয় হওয়া প্রয়োজন এমন বিষয়;
- ii) নিরাপত্তা বিষয়ক শিক্ষা, প্রশিক্ষণ ও সচেতনতা সৃষ্টির জন্য অনুসরণীয়;
- iii) প্রতিষ্ঠানের কার্যক্রমের ধারাবাহিকতা রক্ষার জন্য প্রয়োজনীয়;
- iv) তথ্য নিরাপত্তা পলিসি ভঙ্গের পরিণতি সম্পর্কে ব্যাখ্যার জন্য প্রয়োজনীয়।

(ঙ) তথ্য নিরাপত্তা সংক্রান্ত ইপিডেন্টের রিপোর্টকরণসহ তথ্য নিরাপত্তা ব্যবস্থাপনার জন্য সাধারণ ও বিশেষ দায়-দায়িত্বের সংজ্ঞা নিরূপণ।

(চ) তথ্য নিরাপত্তা পলিসির সহায়ক কাগজপত্রের উৎস, বর্ণনা যথা-একটি বিশেষ তথ্য ব্যবস্থার জন্য নির্দেশনাবলি এবং কার্যপ্রণালী অথবা তথ্যের নিরাপত্তা বিষয়ক আইন-কানুন যাহা ব্যবহারকারীদের মানিয়া চলিতে হইবে।

(২) এই তথ্য নিরাপত্তা পলিসিকে অবশ্যই সংস্থার ভিতরে সকল ব্যবহারকারীর কাছে এমনভাবে পৌঁছাইয়া দিতে হইবে যাহাতে আগ্রহী পাঠক ও ব্যবহারকারীগণ ইহা সহজে বুঝিতে পারে।

(৩) তথ্য নিরাপত্তা পলিসির নমুনা ছক

১. প্রস্তাবনা	৯. ঝুঁকি ব্যবস্থাপনা
২. সংজ্ঞা	১০. নিরাপত্তা নিয়ন্ত্রণ
৩. ভূমিকা	১১. নিরাপত্তা পলিসিসমূহ, ইহাদের মূলনীতি, মানদণ্ড ও এইগুলির যথাযথ অনুসরণ
৪. উদ্দেশ্য	১২. ইন্সিডেন্ট ব্যবস্থাপনা
৫. ক্ষেত্র/আওতা	১৩. পলিসি সম্পর্কিত সচেতনতা এবং তথ্য নিরাপত্তা বিষয়ক প্রশিক্ষণ
৬. পলিসি বাস্তবায়ন ও পরিবীক্ষণ	১৪. তথ্যসূত্রের বর্ণনা (নির্দেশনাপত্র/পদ্ধতি/পরিশিষ্ট)
৭. তথ্য সম্পদ ও শ্রেণিকরণ	
৮. ভূমিকা ও দায়দায়িত্ব	

১৯। পরিশিষ্ট-খ: তথ্যসূত্র

Appendix B: References

(১) CoBIT: IT Governance Framework

(২) ITIL: IT Services Management

(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 management Measurement

(৮) ISO/IEC 27005:2008, Information security risk management

(৯) ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems

(১০) ISO/IEC 27007, Guidelines for information security management systems auditing

(১১) ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

(১২) ISO 31000:2009 Risk management Principles and guidelines

(১৩) ISO/IEC TR 18044, Information technology Security techniques Information security incident management

২০। পরিশিষ্ট-গ: শব্দসংক্ষেপ

১. এএস: অস্ট্রেলিয়া স্ট্যান্ডার্ড (AS : Australia Standard)

২. এনজিএস: নিউজিল্যান্ড স্ট্যান্ডার্ড (NZS : New Zealand Standard)

৩. এপিটি: এ্যাডভান্সড পারসিসটেন্ট থ্রেট (APT: Advanced Persistent Threat)

৪. বিসিসি: বাংলাদেশ কম্পিউটার কাউন্সিল (BCC : Bangladesh Computer Council)

৫. বিটিআরসি: বাংলাদেশ টেলিকমিউনিকেশন রেগুলেটরি কমিশন (BTRC : Bangladesh Telecommunication Regulatory Commission)

৬. সিসিএ: কন্ট্রোলার অব সার্টিফায়িং অথরিটি (CCA : Controller of Certifying Authorities)

৭. সিওবিআইটি: কন্ট্রোল অবজেকটিভস ফর ইনফরমেশন এ্যাণ্ড রিলেটেড টেকনোলজি (CoBIT : Control Objectives for Information and Related Technology)

৮. ডিডিওএস: ডিস্ট্রিবিউটেড ডিনায়েল অব সার্ভিস (DDoS : Distributed Denial of Service)

৯. ইউইউ: ইউরোপিয়ান ইউনিয়ন (EU : European Union)

১০. এফএফআইইসি: ফেডারেল ফিন্যান্সিয়াল ইন্সটিটিউশনস এক্সামিনেশন কাউন্সিল (FFIEC : Federal Financial Institutions Examination Council)

১১. আইসিটি: ইনফরমেশন এ্যাণ্ড কমিউনিকেশন টেকনোলজি (ICT : Information and Communication Technology)

-
১২. আইডিএস: ইন্ট্রুশন ডিটেকশন সিস্টেম (IDS : Intrusion Detection System)
১৩. আইইসি: ইন্টারন্যাশনাল ইলেক্ট্রো টেকনিক্যাল কমিউনিকেশন (IEC : International Electro-technical Communication)
১৪. আইইটিএফ: ইন্টারনেট ইঞ্জিনিয়ারিং টাস্ক ফোর্স (IETF : Internet Engineering Task Force)
১৫. আইপিএসঃ ইন্ট্রুশন প্রিভেনশন সিস্টেম (IPS :Intrusion Prevention System
IS :Information)
১৬. আইএসএমএসঃ ইনফরমেশন সিকিউরিটি ম্যানেজমেন্ট সিস্টেম (ISMS :
Information Security Management System)
১৭. আইএসওঃ ইন্টারন্যাশনাল অর্গানাইজেশন ফর স্ট্যান্ডার্ডস (ISO: International
Organization for Standards)
১৮. আইটি : ইনফরমেশন টেকনোলজি (IT : Information Technology)
১৯. আইটিআইএল : ইনফরমেশন টেকনোলজি ইনফ্রাস্ট্রাকচার লাইব্রেরী (ITIL :
Information Technology Infrastructure Library)
২০. এলএএন : লোকাল এরিয়া নেটওয়ার্ক (LAN : Local Area Network)
২১. ওইসিডি : অর্গানাইজেশন ফর ইকোনমিক এ্যান্ড কো-অপারেশন ডেভেলপমেন্ট
(OECD : Organization for Economic Cooperation and Development)
২২. পিসিঃ পার্সোনাল কম্পিউটার (PC: Personal Computer)
২৩. পিডিসিএ : প্ল্যান-ডু-চেক এ্যান্ড সাইকেল (PDCA : Plan-Do-Check Act Cycle)
২৪. পিকেআই : পাবলিক কী ইনফ্রাস্ট্রাকচার (PKI : Public Key Infrastructure)
২৫. আরএফসি : রিকয়েস্ট ফর কমেন্ট (RFC : Request For Comment)
২৬. ইউএসএ : ইউনাইটেড স্টেটস অব আমেরিকা (USA : United States of America)

1. Preamble

Government of the People's Republic of Bangladesh intends to materialize the Vision 2021: Digital Bangladesh. To achieve this vision, all government agencies will be brought under the e-governance framework. Different government Ministries/Divisions, Departments/agencies and their subordinate bodies have started implementing e-governance. The intention is to improve and ease the government work process and to increase the productivity of the government. While doing this, it is required to digitize the government information, to process and store those digitized information in a manner so that the information doesn't get lost or the information is not manipulated. It is very important to consider information

security for a government while implementing e-governance. This document is a guideline to help government agencies to formulate their own Information Security Policy to protect their information in the cyber space. In recent past, Bangladesh has faced a number of cyber attack incidents in the form of web defacement, information damage, information theft, Distributed Denial of service, etc, due to lack of information protection procedure, weak and unmanaged security controls and lack of expertise because of under skilled personnel. Currently, there are no sufficiently enforceable preventive, reactive, detective and administrative security measures against the above mentioned threats to protect digitized government resources. So it is necessary to have a proper security policy and implementation mechanism in place. This policy will act as a guideline document for government agencies who intends to formulate their own Information Security Policy for the protection of their information in the cyber space.

2. Introduction

(1) Information is the most valuable asset for an agency. Information has different dimension in terms of accessibility. Some information is public where as some are confidential. Depending on the degree of confidentiality, information has several level of accessibility as well. Such as there are information which are open for public access without any authentication, some are accessible with single factor authentication, some require multi factor authentication whereas some are private within the organization, some are highly confidential that only a group of people in an organization has access. So it is very important for an agency to have clear understanding about its information and its accessibility. Before preparing an Information Security Policy it is recommended for an agency to classify their information through proper assessment.

(2) Internet is an open platform for all to access information. Internet technology and other technologies like handheld devices, mobile devices, tablet PCs, wireless technologies are making information easily accessible and affordable. There may be some situation when information can be used as weapon to make chaos in a country. So it is the duty of an agency to take care of its own information in the internet. Apart from information in internet, the agency should also be aware of the information that may have different state such as information that's moving in the intranet or LAN or in the cloud or simply stored in an internal database or in a PC.

(3) This guideline covers :

- a. Brief illustration of different terminology that's important to know while preparing Information Security Policy,

-
- b. Objective of this guideline,
 - c. Scope of this guideline,
 - d. Information classification and different state of information,
 - e. Roles and responsibility of the information owner and information custodian,
 - f. Information security strategy,
 - g. Identification of probable risks, threats and vulnerabilities,
 - h. Assessment of risks, threats and vulnerabilities,
 - i. Procedure to set security controls to protect information,
 - j. Legal issues of information security,
 - k. Standards to follow to establish Information Security Management System (ISMS),
 - l. Importance of auditing for information security,
 - m. Monitoring and improving,
 - n. Certification as an agency,
 - o. Procedures for incident handling and disaster recovery,
 - p. Backup & restore mechanism,
 - q. Business continuity plan,
 - r. Sample Information security policy.

3. Guideline Governance and Enforcement

(1) Ministry of ICT on behalf of the Government of Bangladesh will have the ownership of this guideline. Ministry of ICT will monitor the implementation of this guideline. Bangladesh Computer Council, Office of the CCA and Bangladesh Telecommunication Regulatory Commission (BTRC) will jointly coordinate the implementation of this guideline.

(2) All the agencies of Bangladesh Government are to develop their own Information Security Policy and implement accordingly within six (6) months of the commencement of the guideline. Any query regarding this document can be forwarded either to Ministry of ICT or to BCC. If any agency requires assistance for preparing their Information Security Policy, It may request support from BCC.

4. Definition

(1) **Agency** : Agency includes ministry/division, departments and subordinate bodies of the Government of Bangladesh

-
- (2) **Asset** : Anything that carries value to an agency.
- (3) **Attack** : Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
- (4) **Authentication** : Provision of assurance that a claimed characteristic of an entity is correct.
- (5) **Authenticity** : Property that an entity is what it claims to be.
- (6) **Availability** : Information Systems available to users at any given or specified period of time and being accessible and usable upon demand by an authorized entity.
- (7) **Business Continuity** : Processes or Procedures for ensuring continued business operations.
- (8) **Confidentiality**: Information is not made available or disclosed to unauthorized individuals, entities, systems or processes.
- (9) **Certification**: Certification is something provided by any standard bodies or by some form of external review after evaluating an agency's information system infrastructure and information security management system.
- (10) **Classified Information**: It refers to the categories of information classified in accordance with the Security Regulations.
- (11) **Control**: It means managing risk in an agency including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management related, or legal nature. Control is also used as a synonym for safeguard or countermeasure.
- (12) **Control objective**: Statement describing what is to be achieved as a result of implementing controls.
- (13) **Corrective action**: Action to eliminate the cause of a detected nonconformity or other undesirable situation.
- (14) **Eavesdropping**: Eavesdropping, an unauthorized access to information, is a kind of network attack by capturing packets while communication/transmission of information.
- (15) **Exploit**: A technique or code that uses a vulnerability to provide system access to the attacker.

(16) **Guideline:** A description that clarifies what should be done and how, to achieve the objectives set out in policies information processing facilities any information processing system, service or infrastructure, or the physical locations housing them.

(17) **Information System:** An electronic information system that processes data electronically through the use of information technology - including but is not limited to: computer systems, servers, workstations, terminals, storage media, communication devices, network resources and Internet.

(18) **Integrity:** When authorized persons are allowed to make changes to the information stored or processed by Information Systems in any aspects.

(19) **Information security:** Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

(20) **Information Security (IS) Policy:** A documented list of management instructions that describe in detail the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorized disclosure, modifications or destruction.

(21) **Information security event:** An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

(22) **Information security incident:** An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

(23) **PKI:** PKI is a framework that consists of hardware, software, policies, and procedures for managing keys and certificates.

(24) **Policy:** Overall intention and direction as formally expressed by management.

(25) **Risk analysis:** Systematic use of information to identify sources and to estimate the risk.

(26) **Risk assessment:** Overall process of risk analysis and risk evaluation.

(27) **Risk evaluation:** Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

- (28) **Risk management:** Coordinated activities to direct and control an organization with regard to risk.
- (29) **Risk treatment:** Process of selection and implementation of measures to control or minimize risk.
- (30) **Social engineering:** Obtaining information from individuals by trickery.
- (31) **Spoofing:** A form of masquerading where a trusted IP address is used instead of the true IP address as a means of gaining access to a computer system.
- (32) **Third party:** That person or body that is recognized as being independent of the parties involved, as concerns the issue in question.

5. Objective

(1) Information is an important asset for an agency as well as for a state. Protecting information is vital to establish and maintain trust among government, citizen and business entities. Information security is the process, involved with the people and technology of an agency, by which that agency protects and secures its information. Information Security Policy defines set of rules and control mechanism to protect information against attacks or threats or misuses or damage or unauthorized access.

(2) The objective of this guideline is—

- a. to help agencies of the Government of Bangladesh to understand the nutshell of Information Security,
- b. to define the methodology to prepare Information Security Policy,
- c. to give them proper guidance to implement Information Security Policy.

6. Scope

All government, semi-government, autonomous agency or public limited company in Bangladesh who wants to prepare their Information Security Policy document, can use this guideline. This is a baseline for them to prepare their policy to protect their information. Any private organization inside Bangladesh can also adopt this guideline.

7. Information Asset

(1) This section will assist the key members of an agency to redefine their idea on agencies information/data. It'll help them to understand how to define different states and classify their information asset. It will also help setting ownership and custody for different information asset. As a result an agency can safeguard the information asset according to the defined roles and responsibilities.

(2) Definition of Information

Information is an asset that, like other important business assets, is essential to an organization's business and consequently be appropriately safe guarded. Broadly defined Information is the basis on which the agency conducts their business. Reliable information supports business capabilities, notably by enabling good decision making. The Government holds information that is operationally, administratively, politically, commercially or personally significant. The government has a fundamental 'duty of care' and legal obligations to protect this information from unauthorized or accidental modification, loss/damages or release. There are moral and ethical considerations in the appropriate handling of information as well.

(3) Information can be in any form. It includes:

- a. documents and papers;
- b. electronic data;
- c. the systems (software, hardware and networks) on which the information is stored, processed or communicated;
- d. intellectual information (knowledge or perceptions) acquired by individuals;
- e. physical items from which information regarding design, components or use could be derived; and
- f. Images, audio or video clips.

(4) Definition of Information Asset

Asset is anything that has a value to the organization, agency or nation. Information is a key asset for an organization. Asset must be kept under protection for ensuring trust among stakeholders who use and own the asset. Asset is very much related to security risks assessment. The first step in assessing security risks is to take stock of enterprise's information assets (e.g. application programs, stored data, reports, product designs and specifications, proposals, business plans, financial records, databases, and other files and documents residing on your organization's computer systems). The objective is to organize the assets, conceptually, into appropriate categories, to help understand them and their boundaries. It is necessary to determine the appropriate owners of the various assets and convince them to take responsibility for evaluating their importance and value.

(5) Asset must be classified for assigning access to that asset. Once the information resources have been identified and developed with appropriate ways of classifying and understanding their perimeters, the next step is to define who

needs access to what information. There are many types of assets including but not limited to the following:

- a. databases and data files, contracts and agreements, system documentation including process, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
- b. application software, system software, development tools, and utilities;
- c. computer equipment, communications equipment, removable media, and other equipment;
- d. computing and communications services;
- e. people, and their qualifications, skills, and experience;
- f. intangibles, such as reputation and image of the organization.

(6) Information is created, processed, stored, archived, and deleted while executing business activities. Examples are database records, mails, source code, paper documents, designs, emails, databases, Process Data, images etc.

(7) An information asset is a definable piece of information, stored in any manner which is recognized as 'valuable' to the organization. The most important and valuable information assets are those underpinning an agency's core or most critical duties, capabilities or goals. The value of information assets is expressed in terms of the potential business consequences for events resulting in loss of confidentiality, integrity and or availability to them. Potential consequences include direct and indirect financial losses (immediate or subsequent), loss of revenue, failure to meet service obligations or reputational loss. Indirect consequences of a security failure also have to be considered. Information asset valuation can be done in terms of,

- a. Confidentiality of Information Asset;
- b. Integrity of Information Asset;
- c. Authenticity of Information Asset;
- d. Non-repudiation; and
- e. Availability of Information Asset.

(8) Different State of Information

As mentioned earlier information has different form of presence. It has different state as well. It is very important for an agency to consider those states while developing their policy for Information Security. Common states of information are:

- a. Information that's been archived (Historical information)

- b. Agencies private information or personnel information stored in database or tape drive or in any media
- c. Regular business information processed in applications
- d. Static and dynamic information in the website of the agency
- e. Communication/correspondence, perception and knowledge
- f. Information that's processed in the Intranet of the agency/government
- g. Information that's processed in the internet of the agency/government
- h. Information that's processed in the extranet

(9) Different state of information needs different security mechanism. This shall be done considering the importance of the information and classifying information as required. It is much easier and convenient to impose security controls for same group of information depending on their nature of importance. Every agency shall find out the states of its information and define the security policy along with the classified information.

(10) Information Classification

Information of different types needs to be secured in different ways. Therefore a classification system is needed, whereby information is classified, a policy is laid down on how to handle information according to its class. Depending on the classification, security mechanisms are enforced on systems for handling information accordingly. Information classification ensures that information receives an appropriate level of protection. Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

(11) Information can be classified in terms of its value, legal requirements, sensitivity, and criticality to the country or to the agency. Classification systems vary from country to country, agency to agency. In most countries, the common classification has five levels as mentioned below:

- a. Top Secret
- b. Secret
- c. Confidential
- d. Restricted
- e. Public or Unclassified

(12) While classifying information asset, it is recommended to check compliance with government laws and regulations. The agency may decide to have its own way of classification with more or less number of levels. But it is the most important job of an agency to analyze their information and define the states and classification. Accordingly, the agency shall impose security controls.

(13) Information Owner

The Information owner is a functional owner responsible for ensuring information classification with different state, proper controls to address confidentiality, integrity, authenticity and availability of information. Information owner has authority and responsibility for controlling production, development, maintenance; using security controls over the asset; placing appropriate level of protection; reviewing the information classification, security controls, access restrictions periodically for making cost-benefit decisions essential to ensure accomplishment of organizational mission objectives.

(14) Information Custodian

The Information custodian is a person designated by the owner to be responsible for protecting information by maintaining safeguards and controls established by the owner; he will take prior approval if necessary before sharing information. A custodian is also responsible to perform regular backup and data validity testing activities, data restoration from backups periodically, implement access control as defined by information owner. One custodian should be assigned for each information asset. The custodian remains ultimately responsible for the security of the asset and should be able to determine that any delegated responsibility has been discharged correctly.

(15) Roles and responsibilities

Agencies are responsible and accountable for appropriately safeguarding the information assets in their custody. Agencies are best able to gauge the significance and worth of their information assets, the risks to them and the appropriate measures to safeguard them. The approach is to achieve and maintain appropriate protection of organizational assets. To accomplish this goal, all assets should be accounted for and have a nominated owner. Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The information/asset owner has the responsibility to define the classification of information/asset, periodically review it, and ensure that it is kept up to date and at the appropriate level of security controls. The implementation of specific controls may be delegated by

the owner as deemed appropriate but the owner remains responsible for the proper protection of the information assets. One of the very important obligations for any agency is not to outsource the responsibility of their information, i.e. responsibility for the security of information assets should be kept always within the agency owning that.

(16) Archiving of Information Asset

Continuous accumulation of information will be voluminous and may go beyond the manageable limit resulting difficulties in handling information for its optimum utilization. Therefore obsolete, duplicate, redundant and unnecessary information may be destroyed or archived. While destroying any information an agency must get proper approval from information owner and custodian for destroying, and they must maintain a log mentioning reason for destruction. In case of archival, similar to archival of paper and files, an agency must consider archival of electronic information asset. Depending on the importance of information asset agency may define retention period of information asset. An agency must follow Section 9 of ICT Act 2006 and other relevant law before defining the retention period of electronic information.

(17) Actions according to this Section

The tasks defined throughout section 7, are the prior tasks of an agency that should be structured properly in their Information Security Policy. As a whole, this is called information gathering and information asset management. Steps towards accomplishing this include:

(a) **Information classification and state**

Information should be analyzed and classified in terms of its value, legal requirements, sensitivity, and criticality to the organization. After classification, the states of those classified information must also be defined.

(b) **Inventory of Information assets**

All information assets should be clearly identified and an inventory of all important assets should be drawn up and maintained. An agency should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned.

(c) Information labeling and handling

An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization. Procedures for information labeling need to cover information assets in physical and electronic formats.

(d) Ownership of Information assets

All information and assets associated with information processing facilities should be owned by a designated part of the organization. The asset owner should be responsible for:

- a. ensuring that information and assets associated with information processing facilities are appropriately classified;
- b. defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

(e) Acceptable use of Information assets

Rules for the acceptable use of information assets associated with information processing facilities should be identified, documented, and implemented. All employees, contractors and third party users should follow rules.

(f) Responsibilities

Owners, custodian and others should be identified and assigned with the responsibility of information asset management within an agency. Their responsibilities shall be clearly defined and reviewed periodically for seamless protection of information asset. Archival of information and retention period of information asset must also be considered while defining the responsibilities.

8. Strategy for Information Security

(1) Agency before preparing its Information Security Policy should set a plan for integrating process, people, technology, procedures to safeguard its information from threats. The strategy should be reviewed periodically to mitigate newer threats and vulnerabilities in the area of information security. This section will assist the agency to understand the best practices of Information Security Strategy in the globe and will help them prepare their own strategy or adopt available best practices.

(2) Preparing Strategy

It is important to understand the best practices to prepare own strategy but it is not always rational to adopt the best practices only. Accepting best practices only may leave the policy strategy unworkable and unrealistic. So, it's always recommended to prepare strategy blending the real world and best practices as required by an agency. Information security strategy has the following stages:

(a) Stage 1: Objective

There must be an objective for an organization/agency to adopt information security strategy. For most organization/agency the objective is to safeguard their information from threats in the cyber space. Threats of information theft or loss may disrupt the goal and productivity of an agency. So the agencies should set their objective to protect their information from threats.

(b) Stage 2: Understanding

Before starting formulation of the security policy for an agency, it is required to have a thorough understanding of the agency. It is also required to consider the goals and direction of the agency. The policy that is going to be developed must also conform to existing policies, rules, regulations and laws that the agency is subject to. In this stage, before developing the policy, it is also required to gather information to identify the information assets; to identify the risks, vulnerabilities & threats; to identify potential safeguards & controls with associated cost and percentage of risk reduction; and to re-define roles and responsibilities.

(c) Stage 3: Plan

With the gathered information of stage two (2) and considering the objective the agency shall prepare its security policy in this stage. This stage may include procedures, standards, guidelines etc along with the policy. While preparing the security policy it is recommended that the agency should take assistance and check compliance with ISO/IEC 27002: Code of Practice for Information Security Management. While developing the policy, the agency should consider the location of their information asset, whether they are putting it inside their domain or outside. The government agency must keep their information asset inside the country. And it is recommended that the government agencies should keep their information asset in the National Data Center hosted in BCC. Before putting the policy in action, it is recommended to organize consultation among the implementer and stakeholders of the policy. Such consultation will help produce effective security policy.

(d) Stage 4: Implementation

After preparing the policy and other supporting procedures or guidelines, the agency shall educate its personnel and distribute these to all its implementers (management, BOD, employees etc.) and take their agreement that they read & understood the policy and agreed to comply with it. The key to acceptance and compliance with security policies is education. Educating employees on the need for security and keeping them involved in the policy development process is important to keep them from finding ways to avoid policies and rendering them ineffective. Seminars and awareness campaigns help to educate the importance of security, especially on password selection, screen locking, document labeling, and physical security. Helpdesk in the preliminary stage for successful implementation may also be introduced.

(e) Stage 5: Check Compliance

It is always recommended that the agency must develop a method to measure compliance with the policy and check compliance in a periodical basis. This compliance method may include the formation of auditing team to ensure that the policy is enforced. The auditors who are responsible for monitoring compliance with the security policy should be independent of the persons implementing the policy. The policies must be enforced in a strictly manner and noncompliance of the policy is punishable.

(f) Stage 6: Monitoring & Review

It is important to have monitoring and review mechanism for future improvement since new threats are being discovered as time passes by. Monitoring & review includes changes in the organization resulting in new threats. Security controls have to be modified as necessary to mitigate any new threat introduced. Training is vital issue that might need to arrange for performance improvement. As time goes by, it is crucial to maintain the relevancy of the security policies. New policies may be added when necessary.

(3) Actions according to this section

In this section, the strategy for information security is defined. It is the whole life cycle for an agency to work out to develop an Information Security Policy so is to successfully protect their information assets. The stages defined in this section must be followed by agencies to safeguard their valuable information from threats. Actions in previous section (section 7.9) are part of the stages in the strategy defined earlier. The users of this policy guideline are requested not to create any confusion on what to do first. The users, who want to prepare information security policy for their agencies, should start with the stages defined in section 8.1. All other sections are to assist completing these six (6) stages.

9. Risk, Threats and Vulnerabilities

(1) While formulating a security policy every organization or agency should be aware of possible risks that can affect the safety and security of their information asset. The organization or agency should also have clear understanding about threats and vulnerabilities that could damage its information assets. For appropriate safeguard of information assets knowledge about risks, threats and vulnerability is vital. This section will assist an agency to understand and identify and analyze threats, risks and vulnerabilities.

(2) Understanding Risk, Threat and Vulnerability

(a) Risk

The potential (merely “chance”) for loss, damage or destruction of an information asset as a result of a threat exploiting a vulnerability. Reducing the risk of an organization requires risk identification and risk management process to be done periodically. An agency should know major risks that may cause potential loss of their information asset. Reasons for major risks/weaknesses are:

- a. little support for security measures,
- b. information is not classified,
- c. inadequate information security policy operates,
- d. lack of security awareness are there,
- e. weak access control mechanisms exists,
- f. no official policy and no monitoring/intrusion detection or no incident response team are in place,
- g. Operating procedures are not documented,
- h. Employees are not identified adequately, visitors may roam unchecked,
- i. The building is in an earthquake zone;
- j. The building is in a flooded zone or can be affected by flood because of improper water disposal system,
- k. Lack of fire prevention system, etc.

(b) Threat

A threat is a potential cause of an unwanted incident, which may result in harm to a system or organizations' information assets. Threat is anything that can exploit vulnerability, intentionally or accidentally, and causes damage, or destruction of an asset. Threats can occur by natural disaster, intentional or accidental acts originating from inside or outside the agency. Most threats exploit vulnerabilities in information assets or their supporting infrastructure (hardware or software). Typical information security threats that could cause unwanted event include:

- a. unauthorized access,
- b. disclosure of information,
- c. legal threats,
- d. sabotage,
- e. inadequate security awareness,
- f. poor security policy,
- g. fraudulence,
- h. workload,
- i. denial of service,
- j. spoofing,
- k. advanced persistent threat (APT),
- l. applications with bugs,
- m. eavesdropping,
- n. identity,
- o. DNS security threat etc.

(c) Vulnerabilities

Vulnerabilities are flaws or weaknesses associated with an agency's assets or capabilities. Vulnerability is merely a condition or set of conditions that may allow a threat to affect an asset. Therefore, a vulnerability that cannot be exploited by a threat cannot be a security risk. Typically vulnerability results from:

- a. flawed procedures,
- b. under-skilled staff,
- c. incorrectly configured or defective technology.

(d) For a vulnerability to be exploitable it must be known to or discoverable by a threat. This makes it important to follow the ‘need to know’ principle with respect to security related information, and it applies for both people and technology. It also makes it important for an agency to react appropriately when learning of vulnerabilities or vulnerabilities that affect it. However, the most pervasive vulnerability is probably the susceptibility of staff to ‘social engineering’, In such case security awareness for all staff is an important safeguard. Vulnerabilities are classified according to the related assets:

- a. Organizational
- b. Personnel
- c. Environmental
- d. Hardware, software and network
- e. Spatial

(3) Identification of Risk, Threats, and Vulnerabilities Information Security Policy is needed for an agency to protect their information asset from risks (that may cause damage or lose of information asset) caused by threats exploiting certain vulnerabilities. It is always seen that most agencies always mix up the definition of risk, threat and vulnerability. Risk, threat and vulnerability are not terminologies for same meaning. For clear understanding of these three terms, following is a good simple relative definition between information asset, risk, threat and vulnerability:

Information Asset	Threat	Vulnerability	Risk
Information asset is something what agency tries to protect.	Threat is something against what an agency tries to protect their information asset.	Vulnerability is the weakness or gap in the protection efforts made by an agency.	Risk is destruction (or chance of destruction) of an information asset as a result of threat exploiting vulnerability.

It is important for every agency to identify risk, threat and vulnerabilities to their information system and to apply security controls accordingly. Classification of information and state of information will make the job easier for an agency to do the risk assessment and to apply security controls. An agency must define the degree of identified risk factor in terms of severity of the risk. This scaling must be defined in numerical scale from 0 to 10 where 0 is for low and 10 is for high degree.

(4) Risk Management The objective of the risk management process is to identify threats and vulnerabilities and to provide recommendations to ensure protection of information asset. The risk management process can be done with internal or external resources. Area that an agency must consider before risk management process, are:

- a. Network and software design and development,
- b. Change management,
- c. Physical security, Access control,
- d. External vulnerability, Internal vulnerability,
- e. Storage and backup strategies, restoration procedure and testing
- f. Contingency planning/testing (disaster recovery/business continuity),
- g. Information transmission,
- h. Disposal of information assets,
- i. Personnel skill,
- j. incident management history,
- k. Systems audit practices, etc.

(5) An agency must define its risk management process while producing the IS Policy. A model has been developed by a project called CORAS of EU based on AS/NZS 4360:2004 and ISO/IEC 31000:2009 which is a very good and acceptable model for risk management. This model can also be adopted by any agency in Bangladesh or they can develop their own model.

There are 5(five)steps in Risk Management process shown as circle in the figure. The vertical boxes: Monitoring & Review and Communicate & Consult is necessary in every step of risk management process for effectiveness and improvement. The stages in risk management process are:

(6) Establish the context

The purpose of the context establishment is to characterize the target of the analysis and its environment. There could be external, internal and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis is to be defined.

(7) Identify Risk

In this stage, the agency must identify where, when, why and how incident can happen, that is identification of threats. When an incident is triggered by a threat shall be identified as vulnerabilities. While doing this, it is recommended that the classification of information assets is done.

(8) Analyze Risk

This is the stage where an agency will do the risk estimation. Here an agency will identify and evaluate existing controls for security arrangements. Then the agency will determine the consequences and likelihood and the level of risk. This analysis should consider the range of potential consequences.

(9) Evaluate Risk

This is a very important stage to make decision how to treat a risk. In this stage, on the basis of the result of analyzing risks, an agency will map the risks with their associated risk values to decide how to treat them. There might come some risks where no treatment is required. Here the agency will make a priority for treating risk.

(10) Treat Risk

As per the result coming from previous stages, the agency may prepare effective plans and procedures to mitigate the risks. It is always recommended that plans with maximum effectiveness and minimum cost are prepared. Treating risk may include risk avoidance, risk transfer, changing likelihood and consequences of the risk.

(11) Risk Management Template

An agency must prepare a template for its risk management process. And this risk analysis process must be a periodical process over the lifecycle of an agency. Risk assessment template is a simple form with fields that an agency will periodically fill up after completing the risk analysis. In this guideline, a sample template is given below:

Information Asset		Threat Analysis		Vulnerability Analysis		Risk Analysis		Action Plans to mitigate	Remarks
Details	Class & State	Name	Details	Name	Details	Details	Level		

(12) Actions according to this section

This section describes the function related with several stages of Information Security strategy defined in section 8.1, especially in Stage 2: Understanding, Stage 4: Implementation and Stage 6: Monitoring & Review. Risk management is more an action than just a policy. An agency while preparing its Information Security Policy may include the methodology/model of risk assessment along with definition and reasons for having this. The following things are recommended to be included in the methodology/model for comprehensive risk management:

- a. Frequency of Risk Assessment,
- b. Information Gathering,
- c. Threat & Vulnerability Analysis,
- d. Risk Identification,
- e. Risk Analysis & Evaluation,
- f. Risk Treatment,
- g. Monitoring & Review,
- h. Risk assessment Template.

10. Security Controls to protect information

(1) Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks. To help review or design security controls, there should be a classification of controls by several criteria. Security controls can be categorized according to the time, for example:

- a. Before the event, preventive controls;
- b. During the event, detective controls;
- c. After the event, corrective controls.

(2) Security controls can also be categorized according to their nature, for example:

Remarks

- a. Physical controls
- b. Procedural controls
- c. Technical controls
- d. Legal and regulatory or compliance controls

(3) There are a number of best practices in the world where number of information security controls/governance are defined. The following are important among them:

- a. ISO/IEC 27001, ISO/IEC27002
- b. CoBIT 4.1 or above
- c. ITIL V3 or above

(4) The security controls defined in the above best practices are generic and an agency must tailor those standards or best practices as per their need in a cost effective way. It is optimized to consider the classification of information asset while adopting the security controls. There's no need to adopt very rigid security controls for information asset which is not secret. Example of some security controls (taken from ISO/IEC 27002) are as follows:

- a. Personnel Security,
- b. Equipment Control,
- c. Access controls,
- d. Physical and Environmental Protection,
- e. Operational Procedure and responsibilities,
- f. Third party service delivery management,

-
- g. System planning and acceptance,
 - h. Application Security,
 - i. Protection against malicious code,
 - j. Information back-up,
 - k. Network security management,
 - l. Removable Media handling,
 - m. Information exchange/transmission,
 - n. Information disposal,
 - o. Information system security,
 - p. Cryptographic controls,
 - q. Correct processing,
 - r. System files security,
 - s. Monitoring, etc.

It is recommended that agencies will go through ISO/IEC 27002 to know more about these controls. An agency must decide to adopt controls whichever they need to protect their information.

(5) National PKI which is recognized by the ICT Act 2006, is already available in the country and it is under regulation in the Office of the CCA under Ministry of ICT. An agency must use digital signature certificate and PKI enabled applications to ensure their cryptographic controls. Digital Signature Certificate ensures 4 goals of Information Security. These are:

- a. Authenticity (authenticity of information and parties involved in information exchange)
- b. Confidentiality (ensures confidentiality of information using encryption technology)
- c. Integrity (assures information user about the alteration of information)
- d. Non-repudiation (information originator or signer cannot challenge legally that (s)he or they did not sign or originate the information)

11. Legal and Compliance Issues

(1) While preparing the policy the agency must be aware of legal and compliance issues that may be affected if the policy is in place. This is important to consider both internal and external legal and compliance issues to avoid breaches of any law or regulatory obligations and to avoid contradictions with other policies. List of some legal and compliance document that an agency must consider while developing their policy is as follows:

- a. ICT Act 2006 (amended in 2009)
- b. ICT Policy 2009
- c. Right to Information Act, 2009
- d. The Copyright Act-2000 (amended 2005)
- e. The Patent and Design Act-1911
- f. PKI related rules/guidelines for cryptographic controls
- g. National Archives Act, 1983
- h. Cyber Security related laws/guideline/policy
- i. UN conventions/Laws related to internet or cyber security

(2) An agency within the government must formulate such a policy in compliance with national laws, policies and guidelines. In the IS Policy document, an agency must mention the name of the legal documents and other policies/guidelines/standards the policy complies with. An agency must consider that Service Level Agreement (SLA) is in place before taking any services from a vendor or from any other government agency related to ICT services (Hardware, Software, Network or any other information system)

12. Standards and Guideline

The Information Security Policy of an agency does not define any step by step procedures to implement the policy and does not explain any standard the agency is following for the successful implementation of the policy. Standards and guidelines come when the policy is in place. But there must be some guidance in the policy document so that the agency must set the standards and guideline they are going to follow in every stage of protecting their information asset. There may be number of guidelines and standards under a policy document depending on the requirement.

13. Information System Audit and Certification

(1) Agencies which handle critical information system infrastructure, must go through IS audit periodically. The auditor in this case can be internal or external or both. IS audit is very significant to minimize disruptions in operational procedures and to improve performance. IS Audit is part of Stage 6: Monitoring & Review of Information Security strategy.

(2) Certification is something provided by some form of external review by a third party to an agency after evaluating its information system infrastructure and information security management system. The evaluation criteria are always maintained by the standard bodies. Certification gives assurance about an agency to internal and external stakeholders. If an agency wants to get certified in compliance with ISO/IEC 27001, it should check the evaluation criteria from ISO/IEC 27007 beforehand. Bangladesh Computer Council (BCC) as per their rules of business may start certification activities for the agencies implementing ISMS. Quality certification enables organized working environment and allows the agencies to improve their performance.

14. Incident Management

(1) An information security incident is indicated by a single or a series of unwanted or unexpected information security events that make a significant probability of compromising business operations under threatening information security. In the area of Information Security, it is very crucial to consider incident management plan before an incident occurs. No one can exactly know beforehand when and how an incident is coming to impede the business process. Information security incidents may occur at any time. It is very important to establish robust and effective processes to deal with incident.

(2) Incident can be natural or human driven. In both cases, effective incident management depends on how well the management is responding to an incident. In case of natural incident, for example, in case of flood or fire or earthquake or any type of natural calamity it is recommended that one should start with recovery of the information system for business continuity.

(3) Incident can be driven by human intervention in a form of attack. In case of human driven occurrences, Information security incident shall be reported through appropriate management channels as quickly as possible. Internal or external expert or Information Security Incident Response Team must be involved after an incident to investigate and report properly. It is also important to know by all the internal employees to leave the evidence unchanged after an incident has occurred. After successful investigation of an incident, it should be recorded for improvement in the risk management system. And the assessment report on incident must be forwarded to the management for taking necessary actions as deemed necessary.

(4) In the Information Security Policy document there must be some direction of incident management. It is suggested for every agency to go through ISO/IEC TR 18044:2004 for better understanding of Incident Management.

15. Business Continuity Plan

(1) To counteract interruptions to business activities by effects of major failures of information systems or disasters and to ensure the timely resumption of activities, a business continuity management process should be implemented. It is important to minimize the impact of disaster on the organization and to recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) at an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

(2) Information security should be an integral part of the overall business continuity process, and other management processes within the organization. Business continuity management should include controls to identify and reduce risks. In addition to the general risks assessment process, limiting the consequences, and ensuring the availability of information required for business processes shall be considered. Steps in Business continuity plan (as per ISO/IEC 27002) are as follows:

- a. Including information security in the business continuity management process;
- b. Business continuity and risk assessment;
- c. Developing and implementing continuity plans including information security;
- d. Business continuity planning framework;
- e. Testing, maintaining and re-assessing business continuity plans;

It is suggested to every agency to follow ISO/IEC 27002 for preparing a robust and effective business continuity plan. And there must be indication of using that standard in the Information Security Policy document.

16. Monitoring & Improvement

(1) It is important to monitor and review the information security policy for improvement. There are several phases of Information security strategy defined in section 8, monitoring is needed in every phase to improve service quality of that phase. The monitoring discussed here is different from what is defined in Stage 6: Monitoring & Review of Section 8. This is the monitoring applicable for the policy. The objective of this monitoring is to understand how the policy is implemented by the agency, what are the challenges or obstacles of implementation, what are the changes and actions required for improving the policy and whether any modification is needed in the policy document in view of any significant change in the information security or the management context.

(2) There should be some direction in the policy document about monitoring (e.g. who will monitor, frequency of monitoring, whom to report, what are the monitoring results, who are the stakeholders for consultation to improve the policy, etc).

17. National Cyber Security Strategy

It is important for an agency to be aware of the cyber security risk, threat and vulnerability of information. Apart from this guideline, a National Cyber Security Strategy needs to be formulated. Moreover, a separate agency may be established in future for addressing cyber security and information security issues which may be titled as “Bangladesh National Information Security Agency, (BNISA)”.

18. Appendix A: Template of Information Security Policy

(1) The information security policy document should state management commitment and set out the organization’s approach to managing information security. The policy document should contain:

- (a) A definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;
- (b) A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;
- (c) A framework for setting control objectives and controls, including the structure of risk assessment and risk management;
- (d) A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:
 - i) Compliance with legislative, regulatory, and contractual requirements;

- ii) Security education, training, and awareness requirements;
 - iii) Business continuity management;
 - iv) Consequences of information security policy violations;
 - (e) A definition of general and specific responsibilities for information security management, including reporting information security incidents;
 - (f) References to documents that may support the policy, e.g. guidelines and procedures for specific information systems or security rules users should comply with.
- (2) This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader and users.

(3) Sample Outline of an IS Policy:

I. Preamble	IX. Risk management
II. Definitions	X. Security Controls
III. Introduction	XI. Security policies, principles, standards, and Compliance
IV. Purpose	XII. Incident Management
V. Scope	XIII. Policy Awareness and Training on Information Security
VI. Policy Governance & Monitoring	XIV. Reference Documents
VII. Information Asset and Classification	(Guideline/Procedure/Appendix)
VIII. Roles & Responsibilities	

19. Appendix B: References

- (1) CoBIT: IT Governance Framework
- (2) ITIL: IT Services Management
- (3) ISO/IEC 27000:2009, Information security management systems-Overview and vocabulary.
- (4) ISO/IEC 27001:2005, Information security management systems-Requirements.
- (5) ISO/IEC 27002:2005, Code of practice for information security management.
- (6) ISO/IEC 27003, Information security management system implementation guidance.

- (7) ISO/IEC 27004, Information security management - Measurement.
- (8) ISO/IEC 27005:2008, Information security risk management.
- (9) ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems
- (10) ISO/IEC 27007, Guidelines for information security management systems auditing.
- (11) ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- (12) ISO 31000:2009 – Risk management - Principles and guidelines
- (13) ISO/IEC TR 18044. Information technology- Security techniques- Information security incident management.

20. Appendix C: Acronyms

1. AS/NZS Australia/New Zealand Standard
2. APT Advanced Persistent Threat
3. BCC Bangladesh Computer Council
4. BTRC Bangladesh Telecommunication Regulatory Commission
5. CCA Controller of Certifying Authorities
6. CoBIT Control Objectives for Information and Related Technology
7. DDoS Distributed Denial of Service
8. EU European
9. FFIEC Federal Financial Institutions Examination Council
10. ICT Information and Communication Technology
11. IDS Intrusion Detection System
12. IEC International Electro technical Commission
13. IETF Internet Engineering Task Force
14. IPS Intrusion Prevention System
15. IS Information Security
16. ISMS Information Security Management System

17. ISO	International Organization for Standards
18. IT	Information Technology
19. ITIL	Information Technology Infrastructure Library
20. LAN	Local Area Network
21. OECD	Organization for Economic and Cooperation Development
22. PC	Personal Computer
23. PDCA	Plan-Do-Check-Act Cycle
24. PKI	Public Key Infrastructure
25. RFC	Request for Comment
26. USA	United States of America