

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 বদ্ধপরিকর। 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 তথ্য 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 স্চ্ছ ধারণা থাকা অত্যাৱশ্যক। 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 পরিদ্রাণের 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 রাখিয়াছে 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 প্রমান্যতা: 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 যুঁকি 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 অননুমোদিত 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।