গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
ডাক, টেলিযোগাযোগ ও তথ্য প্রযুক্তি মন্ত্রণালয়
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ
www.ictd.gov.bd

প্রজ্ঞাপন

তারিখ: ....., ১৪২৯ বঙ্গাব্দ/ ....., ২০২২ খ্রিষ্টাব্দ

প্রস্তাবনা

যেহেতু ডিজিটাল নিরাপত্তা আইন, ২০১৮ এবং তদধীন প্রণীত বিধিমালার বিধান অনুসারে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা নিশ্চিতকরণ, উহাদের তত্ত্বাবধান ও রক্ষণাবেক্ষণের মানদন্ড নির্ধারণ এবং উহা পরিদর্শন ও পরিবীক্ষণের দায়িত্ব ডিজিটাল নিরাপত্তা এজেন্সির উপর ন্যস্ত করা হইয়াছে; এবং

যেহেতু ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি-৩ এ ডিজিটাল নিরাপত্তা এজেন্সিকে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা ব্যবস্থা সুরক্ষার জন্য অনুসরণীয় গাইডলাইন প্রণয়নের জন্য ক্ষমতা প্রদান করা হইয়াছে;

সেহেতু ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি-৩ এর দফা (খ) ও (গ), বিধি ৭, ১১, ১২ ও ১৭ এর সহিত পঠিতব্য, এ প্রদত্ত ক্ষমতাবলে ডিজিটাল নিরাপত্তা এজেন্সি নিম্নরূপ গাইডলাইন প্রণয়ন করিল, যথা:-

অংশ-১: প্রারম্ভিক

১। শিরোনাম, প্রয়োগ ও প্রবর্তন:

(১) এই গাইডলাইন গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা সুরক্ষা গাইডলাইন, ২০২২ নামে অভিহিত হইবে।

(২) এই গাইডলাইনের বিধানাবলি আইনের ধারা ১৫ এর অধীন ঘোষিত সকল গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ক্ষেত্রে প্রযোজ্য হইবে।

(৩) ডিজিটাল নিরাপত্তা এজেন্সি, আদেশ দ্বারা, যে তারিখ নির্ধারণ করিবে সেই তারিখে এই গাইডলাইন কার্যকর হইবে।

২। সংজ্ঞা:

(১) বিষয় বা প্রসঙ্গের পরিপন্থী কোনো কিছু না থাকিলে, এই গাইডলাইনে-

(ক) "আইন" অর্থ ডিজিটাল নিরাপত্তা আইন, ২০১৮ (২০১৮ সনের ৪৬ নং আইন);

(খ) "আক্রম্যতা (Vulnerability)" অর্থ কম্পিউটার সিস্টেমের দুর্বলতা, যাহার সুযোগ গ্রহণ করিয়া উক্ত সিস্টেমের বিশ্বস্থতা বা গোপনীয়তা (Confidentiality), অখন্ডতা বা শুদ্ধতা (Integrity) এবং লভ্যতাকে (Availability) নেতিবাচকভাবে প্রভাবিত করা যায়;

(গ) "এজেন্সি" অর্থ আইনের ধারা ৫ এর অধীনে গঠিত ডিজিটাল নিরাপত্তা এজেন্সি;

(ঘ) "কম্পিউটার সিস্টেম" অর্থ আইনের ধারা ২(ঙ) তে সংজ্ঞায়িত কম্পিউটার সিস্টেম;

(ঙ) "গুরুত্বপূর্ণ তথ্য পরিকাঠামো" অর্থ আইনের ধারা ২(ছ) এ সংজ্ঞায়িত গুরুত্বপূর্ণ তথ্য পরিকাঠামো;

(চ) "ডিজিটাল ডিভাইস" অর্থ আইনের ধারা ২(ঞ) তে সংজ্ঞায়িত ডিজিটাল ডিভাইস;

(ছ) "ডিজিটাল নিরাপত্তা" অর্থ আইনের ধারা ২(ট) তে সংজ্ঞায়িত ডিজিটাল নিরাপত্তা;

(জ) "ডিজিটাল নিরাপত্তার ঘটনা" অর্থ ডিজিটাল নিরাপত্তা বিধিমালা ২০২০ এর ২(খ) তে সংজ্ঞায়িত ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনা;

(ঝ) "ডিজিটাল স্বাক্ষর" অর্থ তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ ধারা ২(১) এ সংজ্ঞায়িত ইলেকট্রনিক স্বাক্ষর।

(ঞ) "তথ্য প্রযুক্তি" অর্থ পরস্পর সংযুক্ত এমন একটি ব্যবস্থা যাহাতে তথ্যে প্রবেশগম্যতাসহ তথ্য সংরক্ষণ, প্রক্রিয়াজাতকরণ ও বিশ্লেষণ বা প্রেরণ করা হয়;

(ট) "দুর্যোগ পুনরুদ্ধার পরিকল্পনা (Disaster Recovery Planning) অর্থ তথ্য প্রযুক্তি বা কম্পিউটার সিস্টেম ব্যাহত হইবার ক্ষেত্রে যে পদ্ধতিতে উহার সক্ষমতা পুনরুদ্ধার করা হয়;

(ঠ) "দূর নিয়ন্ত্রণ প্রবেশ (Remote Access)" অর্থ কোনো ব্যবহারকারী কর্তৃক বহিঃস্থ নেটওয়ার্ক যোগাযোগের মাধ্যমে গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রবেশ;

(ড) "দূর নিয়ন্ত্রিত সুবিধাদি (Remote Access facility)" অর্থ দূর নিয়ন্ত্রণের মাধ্যমে প্রবেশের সক্ষমতা রহিয়াছে এমন কম্পিউটার বা কম্পিউটার সিস্টেম;

(ঢ) "দূর নিয়ন্ত্রিত কম্পিউটার বা কম্পিউটার সিস্টেম" অর্থ গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দূর নিয়ন্ত্রিত কোনো কম্পিউটার বা কম্পিউটার সিস্টেম, এবং উক্ত পরিকাঠামোর সহিত সংযোজিত দূরনিয়ন্ত্রিত সুবিধাদিও ইহার অন্তর্ভুক্ত হইবে;

(ণ) "নেটওয়ার্ক নিরাপত্তা (Network Security)" অর্থ কম্পিউটার নেটওয়ার্ক বা কম্পিউটার সিস্টেমের নিরাপত্তা;

(ত) "নেটওয়ার্ক জোন" অর্থ কম্পিউটার নেটওয়ার্কের যৌক্তিকভাবে বিভাজিত অংশ;

(থ) "প্যাচ" অর্থ বিশেষ ধরনের প্রোগ্রাম যাহা সফটওয়্যার অথবা অপারেটিং সিস্টেমের চিহ্নিত ঘাটতি বা সীমাবদ্ধতা দূর করিয়া প্রোগ্রামের কার্যকরতা, ব্যবহারযোগ্যতা বা কর্মক্ষমতা উন্নত করিয়া থাকে;

(দ) "পেনিট্রেশন টেস্টিং" অর্থ অনুসন্ধানের মাধ্যমে প্রাপ্ত তথ্যের ভিত্তিতে কম্পিউটার সিস্টেম, নেটওয়ার্ক বা এ্যাপ্লিকেশনের নিরাপত্তা মূল্যায়নের জন্য অনুমোদিত প্রক্রিয়া;

(ধ) "বিধিমালা" অর্থ আইনের অধীনে প্রণীত ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০;

(ন) "মহাপরিচালক" অর্থ ডিজিটাল নিরাপত্তা এজেন্সির মহাপরিচালক;

(প) "ম্যালওয়্যার" অর্থ আইনের ধারা ২(ন) তে সংজ্ঞায়িত ম্যালওয়্যার;

(ফ) "সিকিউরিটি বেইজলাইন কনফিগারেশন স্ট্যান্ডার্ড" অর্থ তথ্য প্রযুক্তির বা অপারেশন প্রযুক্তির জন্য লিখিত প্রক্ষেপণমালা যাহা কোনো এক সময় আনুষ্ঠানিকভাবে স্বীকৃত হইয়াছে;

(ব) "সিস্টেম নকশা পুন:নিরীক্ষণ (System architecture review)" অর্থ গুরুত্বপূর্ণ সম্পদ, নেটওয়ার্ক ডিজাইনের দুর্বলতা, সংবেদনশীল উপাত্ত সংরক্ষণ এবং গুরুত্বপূর্ণ আন্তঃসংযোগ ও এ্যাপ্লিকেশন নকশার ক্ষেত্রে, নেটওয়ার্কে সম্ভাব্য হামলা ও আক্রম্যতা চিহ্নিত করিতে এ্যাপ্লিকেশনের ডিজাইন ও নেটওয়ার্ক নকশার পুন:নিরীক্ষণ ও বিশ্লেষণ;

(ভ) "সেবা প্রদানকারী" অর্থ আইনের ধারা ২(ফ) তে সংজ্ঞায়িত সেবা প্রদানকারী।

(২) এই গাইডলাইনে ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞা এই গাইডলাইনে প্রদান করা হয় নাই, সেই সকল শব্দ বা অভিব্যক্তি আইন, বিধিমালা ও তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ এ যে অর্থে ব্যবহৃত হইয়াছে সেই অর্থে প্রযোজ্য হইবে।

অংশ-২: উদ্দেশ্য ও পরিধি

৩। গাইডলাইন প্রণয়নের উদ্দেশ্য ও পরিধি:

(১) গাইডলাইন প্রণয়নের উদ্দেশ্য:

এই গাইডলাইন প্রণয়নের মুখ্য উদ্দেশ্য হইতেছে, গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা নিশ্চিতকরণে উক্ত পরিকাঠামোর কর্তৃপক্ষ কর্তৃক উহাতে উল্লিখিত নূন্যতম সুরক্ষার নীতি-নির্দেশনা বাস্তবায়ন করা।

(২) গাইডলাইনের পরিধি:

এই গাইডলাইন ডিজিটাল নিরাপত্তা আইন, ২০১৮ ধারা ১৫ এর অধীন ঘোষিত সকল গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ক্ষেত্রে প্রযোজ্য হইবে।

অংশ-৩: গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কার্যাবলী, ইত্যাদি

৪। গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কার্যাবলী:

(১) এই গাইড লাইনের অধীন গুরুত্বপূর্ণ তথ্য পরিকাঠামো, অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত কার্য-সম্পাদন করিবে, যথা: -

(ক) ডিজিটাল সুরক্ষা কৌশল বাস্তবায়নের জন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিজস্ব বাজেট বরাদ্দের ব্যবস্থা করা;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো, প্রয়োজনে, ডিজিটাল নিরাপত্তা এজেন্সির পূর্বানুমোদন গ্রহণক্রমে, উহার নিজস্ব কম্পিউটার ইমার্জেন্সি রেসপন্স টিম গঠন করা;

(গ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার তথ্যের সংবেদনশীলতা, প্রকৃতি (Criticality), মান (Value), গোপনীয়তা (Confidentiality) এবং ব্যক্তিগত সুরক্ষার (Privacy) উপর ভিত্তি করিয়া আইনগত প্রয়োজনীয়তা অনুযায়ী তথ্যের শ্রেণিবিন্যাস নির্ধারণ করা;

(ঘ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে ব্যবহৃত হার্ডওয়্যার, সফটওয়্যার সম্মিলিত সিস্টেম পরিসম্পদের জন্য উপযুক্ত কর্তৃপক্ষের স্বীকৃতি (Accreditation) এবং সনদ (Certification) প্রাপ্তির ব্যবস্থা গ্রহণ করা;

(ঙ) নিয়মিত আক্রম্যতা মূল্যায়ন (Vulnerability Assessment) করিয়া হুমকি এবং পরিসম্পদের কোন প্রকার দুর্বলতা বা ত্রুটি বা প্রতিব্যবস্থার (Countermeasures) অনুপস্থিতি নিরূপণ এবং উক্ত হুমকি, দুর্বলতা বা ত্রুটি, আক্রম্যতা প্রশমনের (Vulnerability Mitigation) ব্যবস্থা করা;

(চ) ঝুঁকি ব্যবস্থাপনা (Risk Management) প্রক্রিয়া দ্বারা প্রাতিষ্ঠানিক প্রতিরক্ষামূলক ব্যবস্থা গ্রহণ করা এবং নিরাপত্তা কর্মসূচির সর্বোচ্চ সক্ষমতা অর্জন করিয়া বাস্তবতার নিরিখে উহার নিরাপত্তার ঝুঁকি নিরসনে সচেষ্ট থাকা;

(ছ) ডিজিটাল নিরাপত্তা সংক্রান্ত ঝুঁকির বিষয়াদি বিবেচনা করিয়া উক্ত ঝুঁকি প্রশমন ও নিরাপত্তা হুমকি প্রতিরোধের ক্ষেত্রে করণীয় বিষয়ে প্রয়োজনীয় শর্ত অন্তর্ভুক্ত করিয়া গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সহিত সংশ্লিষ্ট ভেন্ডর বা সেবা প্রদানকারীর সহিত চুক্তি সম্পাদন করা;

(জ) ডিজিটাল নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে তথ্য প্রযুক্তি নিরীক্ষা কার্য-সম্পাদনের ব্যবস্থা গ্রহণ করা;

(ঝ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনার দায়িত্বে নিয়োজিত মানবসম্পদের এজেন্সি কর্তৃক স্বীকৃত দেশীয় এবং আন্তর্জাতিক আইটি পরিচালনা, আইটি অডিট, আইটি সিকিউরিটি সংক্রান্ত প্রয়োজনীয় প্রশিক্ষণ ও সনদ গ্রহণের ব্যবস্থা করা;

(ঞ) পরিশিষ্ট-১ এ বর্ণিত উত্তম অনুসরণীয় চর্চা অনুসরণ করা;

(ট) সাইবার নিরাপত্তা সম্পর্কিত সকল কার্যক্রমে এজেন্সিকে সকল ধরনের সহায়তা প্রদান করা;

(ঠ) এজেন্সি কর্তৃক সময় সময় প্রদত্ত অন্যান্য কার্যাবলি সম্পাদন করা।

(২) অনুচ্ছেদ (১) এ বর্ণিত কার্যাবলীর অতিরিক্ত হিসাবে গুরুত্বপূর্ণ তথ্য পরিকাঠামো নিজস্ব কর্মক্ষেত্রে (Domain) উক্ত পরিকাঠামোর অভ্যন্তরীণ সাইবার নিরাপত্তা কৌশল, তথ্য ও যোগাযোগ প্রযুক্তি নীতি, পরিকল্পনা এবং এই গাইডলাইনে বর্ণিত সুরক্ষা নির্দেশনার অতিরিক্ত ব্যবস্থা গ্রহণ ও উহার বাস্তবায়ন পদ্ধতি প্রণয়ন করিবে; এইক্ষেত্রে উক্ত পরিকাঠামোর জন্য প্রযোজ্য আইন এবং তদানুযায়ী আইনি ব্যবস্থা গ্রহণের বিষয়সমুহকে অগ্রাধিকার প্রদান করিবে।

৫। গুরুত্বপূর্ণ তথ্য পরিকাঠামো শ্রেণী বিন্যাস:

ডিজিটাল নিরাপত্তা ব্যবস্থার নিরীক্ষা কার্যক্রম সম্পাদনের সুবির্ধাথে, গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহ স্বরাষ্ট্র মন্ত্রণালয় কর্তৃক জারীকৃত কেপিআই নিরাপত্তা নীতিমালা, ২০১৩ এর অধীন নির্ধারিত-

(ক) 'বিশেষ শ্রেণী' এবং '১ক' শ্রেণীভুক্ত প্রতিষ্ঠানসমূহের মধ্যে যে সকল প্রতিষ্ঠান আইনের ধারা ১৫ এর অধীন গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসেবে ঘোষিত হইয়াছে, সেই সকল প্রতিষ্ঠানসমূহ 'প্রথম শ্রেণী',

(খ) **'১খ'** শ্রেণীভুক্ত প্রতিষ্ঠানসমূহের মধ্যে যে সকল প্রতিষ্ঠান আইনের ধারা **১৫** এর অধীন গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসেবে ঘোষিত হইয়াছে, সেই সকল প্রতিষ্ঠানসমূহ 'দ্বিতীয় শ্রেণী',

(গ) **'১গ'** অথবা ২য় শ্রেণীভুক্ত প্রতিষ্ঠানসমূহের মধ্যে যে সকল প্রতিষ্ঠান আইনের ধারা **১৫** এর অধীন গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসেবে ঘোষিত হইয়াছে, সেই সকল প্রতিষ্ঠানসমূহ এই নীতিমালার উদ্দেশ্য পূরণকল্পে, 'তৃতীয় শ্রেণী',

এর গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসেবে গণ্য হইবে এবং যে সকল গুরুত্বপূর্ণ তথ্য পরিকাঠামো কেপিআই শ্রেণীভুক্ত নয় সেই সকল পরিকাঠামো 'তৃতীয় শ্রেণী'র গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসেবে গণ্য হইবে।

অংশ-৪: তথ্য প্রেরণ

৬। গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহের পালনীয় নির্দেশাবলী:

(১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কর্তৃপক্ষ উহার আওতাধীন পরিকাঠামোর একজন কর্মচারিকে ফোকাল পয়েন্ট নির্বাচন করিবে, যিনি উক্ত পরিকাঠামোর পক্ষে ডিজিটাল নিরাপত্তা এজেন্সির সহিত নিয়মিত যোগাযোগের দায়িত্ব পালন করিবে।

(২) ফোকাল পয়েন্টকে অবশ্যই গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কার্যক্রম এবং সংশ্লিষ্ট কারিগরি জ্ঞান সম্পন্ন হইতে হইবে।

(৩) ফোকাল পয়েন্ট ডিজিটাল নিরাপত্তা নিশ্চিতকল্পে যথোপযুক্ত পদক্ষেপ গ্রহণ করিতে পারিবে।

(৪) মহাপরিচালক উক্ত ফোকাল পয়েন্টকে ডিজিটাল নিরাপত্তা সংশ্লিষ্ট তথ্যাদি প্রেরণের জন্য নির্দেশনা প্রদান করিতে পারিবেন, এবং ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ বিধি ৭ অনুযায়ী কোনো নির্দেশনা প্রদান করা হইলে সংশ্লিষ্ট ফোকাল পয়েন্ট এই গাইডলাইনের পরিশিষ্ট-২ এ বর্ণিত ফরমে উহা প্রেরণ করিবে।

(৫) এই অনুচ্ছেদের অধীন অতি সংবেদনশীল তথ্য ডিজিটাল মাধ্যমে প্রেরণের সময় ডিজিটাল স্বাক্ষর ব্যবহার করিতে হইবে।

অংশ-৫: ডিজিটাল নিরাপত্তা

৭। ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা (Incident) অবহিতকরণ:

(১) যেক্ষেত্রে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা সংঘটিত হয়, সেইক্ষেত্রে উক্ত পরিকাঠামোর দায়িত্বপ্রাপ্ত কর্মচারী সংঘটিত ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা সম্পর্কে নিম্নবর্ণিত তথ্য উপ-অনুচ্ছেদ (২) এ বর্ণিত পদ্ধতিতে, লিখিতভাবে, মহাপরিচালককে অবহিত করিবে, যথা: -

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামো ক্ষতিগ্রস্থ হইবার আশঙ্কার বিস্তারিত বিবরণ;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নাম, ফোকাল পয়েন্টের নাম ও যোগাযোগের ফোন নম্বর;

(গ) ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনার প্রকৃতি এবং উহা সংঘটনের সময় ও কিভাবে সংঘটিত হইয়াছে উহার বিস্তারিত বিবরণ;

(ঘ) সংঘটিত ঘটনার ফলাফল বা প্রভাব পর্যবেক্ষণসহ উক্ত পরিকাঠামো ও উহার কম্পিউটার বা কম্পিউটার সিস্টেম ক্ষতিগ্রস্থ হইয়া থাকিলে উহার বিবরণ।

(২) উপ-অনুচ্ছেদে (১) এ উল্লিখিত তথ্য ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা গোচরীভূত হওয়া মাত্রই পরিশিষ্ট-৩ক এ বর্ণিত ফরমে মহাপরিচালক বরাবর অবগত করিতে হইবে।

(৩) উক্ত ঘটনা সংঘটিত হইবার কারণ, উক্ত কারণে পরিকাঠামো বা উহার কম্পিউটার বা কম্পিউটার সিস্টেমের উপর সৃষ্ট প্রভাব এবং এতদসম্পর্কিত অন্যান্য সম্পূরক তথ্য, লিখিতভাবে, মহাপরিচালক কর্তৃক নির্ধারিত সময় বা উক্ত ঘটনা সংঘটিত হইবার ৭ (সাত) কর্মদিবসের মধ্যে, পরিশিষ্ট-৩খ এ বর্ণিত ফরমে নির্ধারিত ইমেইল ঠিকানায় (notify@dsa.gov.bd) প্রেরণ করিতে হইবে।

৮। ডিজিটাল নিরাপত্তা ঝুঁকি নিরূপণ:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা ঝুঁকি নিরূপণের ক্ষেত্রে, বাস্তবতার নিরিখে, জাতীয় সাইবার ঝুঁকি ল্যান্ডস্কেপ (National Cyber Threat Landscape) পর্যালোচনাপূর্বক উক্ত পরিকাঠামোর সংশ্লিষ্ট ডিজিটাল নিরাপত্তার ঝুঁকি নিরূপণ, সম্ভাব্য ঘটনার ফলাফল বা প্রভাব মূল্যায়ন (Impact Analysis) করিয়া উক্ত ঝুঁকি নিরসনে পরিশিষ্ট-৫ এ বর্ণিত ঝুঁকি রেজিস্টারে উহার বিবরণ লিপিবদ্ধকরণের ব্যবস্থা গ্রহণ করিতে হইবে।

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামো ডিজিটাল নিরাপত্তা ঝুঁকি ব্যবস্থাপনার জন্য একটি নিজস্ব নীতিমালা প্রস্তুত করিবে এবং উহাতে অন্যান্য বিষয়ের মধ্যে নিম্নবর্ণিত বিষয়াদি অন্তর্ভুক্ত থাকিবে, যথা: -

(ক) ডিজিটাল নিরাপত্তা ঝুঁকি ব্যবস্থাপনার দায়িত্বে নিয়োজিত কর্মচারীগণের দায়-দায়িত্ব ও তাহাদের জবাবদিহিতা সংক্রান্ত বিষয়াদি;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর পরিসম্পদ চিহ্নিতকরণ;

(গ) উক্ত পরিকাঠামোর ডিজিটাল নিরাপত্তা ঝুঁকি মোকাবেলার রূপরেখাসহ সর্বনিম্ন ঝুঁকির সীমারেখা নির্ধারণ;

(ঘ) ডিজিটাল নিরাপত্তার ঝুঁকি নিরূপণ পদ্ধতি নির্বাচন;

(ঙ) ডিজিটাল নিরাপত্তার ঝুঁকি নিরূপণ পরিবীক্ষণ;

(চ) সিস্টেমের জীবনচক্রের উন্নয়নের নিমিত্ত ডিজিটাল নিরাপত্তা ডিজাইন কাঠামোর (Security by Design Framework) নির্দেশনা প্রদান।

(৩) গুরুত্বপূর্ণ তথ্য পরিকাঠামো, মহাপরিচালক কর্তৃক নির্ধারিত সময়ের মধ্যে, উহার ডিজিটাল নিরাপত্তা ঝুঁকি নিরূপণ ও নিরসন কর্মপরিকল্পনা মহাপরিচালকের নিকট প্রেরণ করিবে।

৯। নিরাপত্তা ঝুঁকি নিরসনে গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কর্মরত কর্মচারীর দায়িত্ব নির্ধারণ:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর প্রয়োজনীয় ডিজিটাল নিরাপত্তার ঝুঁকি চিহ্নিতকল্পে, উক্ত পরিকাঠামোতে দায়িত্ব পালনরত সংশ্লিষ্ট সকলের দায়িত্ব ও কার্যাবলী, এবং তাহাদের অর্পিত দায়িত্বের বিবরণ সুস্পষ্টভাবে লিপিবদ্ধ থাকিতে হইবে, এবং উহাতে, অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত বিষয়সমূহ অন্তর্ভুক্ত থাকিবে, যথা: -

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কর্মরত প্রত্যেক কর্মচারীর কার্যাবলী সুনির্দ্দিষ্টকরণ সংক্রান্ত তথ্য;

(খ) আপদকালীন সময়ে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কর্মচারীদের দায়িত্ব নির্ধারণ;

(গ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো কর্মচারীদের দক্ষতা উন্নয়ন এবং আপদকালীন সময়ে পরিপূর্ণ প্রস্তুতির লক্ষ্যে নিয়মিত অনুশীলনের আয়োজন এবং উহার ফলাফল মূল্যায়ন।

অংশ-৬: ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা শনাক্তকরণ ও প্রতিরোধকরণ

১০। শনাক্তকরণ (Identification):

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সহিত সম্পর্কযুক্ত ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা চিহ্নিতওশনাক্তক্রমে উক্ত হইবার ঘটনা বিশ্লেষণ ও তুলনা করিতে হইবে, এবং ইতোমধ্যে সংঘটিত ডিজিটাল নিরাপত্তা হুমকি বা বিঘ্নিত হইবার ঘটনা চিহ্নিতকরণের উদ্দেশ্যে, প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর একটি কার্য-সম্পাদন ও তথ্য আহরণ প্রক্রিয়ার পদ্ধতি থাকিতে হইবে।

(২) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উপ-অনুচ্ছেদ (১) এর অধীন প্রণীত কার্য-সম্পাদন ও তথ্য আহরণ প্রক্রিয়ার কার্যকরতা নিরূপনার্থ মহাপরিচালক কর্তৃক নির্ধারিত সময়ের মধ্যে অন্ততঃ একবার উহা মূল্যায়ন ও পর্যালোচনা করিবে।

১১। ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনার প্রতিরোধ পরিকল্পনা:

(১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা প্রতিরোধের জন্য একটি সমন্বিত প্রতিরোধ পরিকল্পনা (Response Plan) প্রস্তুত করিবে, এবং উহাতে, অন্যন্য বিষয়ের মধ্যে, নিম্নবর্ণিত বিষয়াদি অন্তর্ভুক্ত থাকিবে, যথা: -

(ক) “সাইবার ইন্সিডেন্ট রেসপন্স টিম” এর গঠন কাঠামো এবং উক্ত টিমের সমস্যগণের দায়িত্ব, কার্যাবলী ও তাহাদের সহিত যোগাযোগের বিবরণ এবং উক্ত ঘটনার প্রতিরোধ সীমা ও পদ্ধতি নির্ধারণ;

(খ) আইন, বিধিমালা ও এই গাইডলাইনের অধীন নিরাপত্তা বিঘ্নিত হইবার ঘটনা সম্পর্কে রিপোর্ট প্রদান পদ্ধতি ও রিপোর্ট প্রণয়ন কাঠামো নির্ধারণ;

(গ) নিরাপত্তা বিঘ্নিত হইবার ঘটনার প্রভাব নিয়ন্ত্রণ এবং উহার পুনরুদ্ধার প্রক্রিয়া কার্যকরকরণ;

(ঘ) ঘটনার কারণ ও উহার প্রভাবের তদন্ত পদ্ধতি নির্ধারণ;

(ঙ) পুনরুদ্ধার প্রক্রিয়া কার্যকর করিবার পূর্বে ঘটনা সম্পর্কিত সাক্ষ্য প্রমাণ সংরক্ষণ পদ্ধতিসহ কম্পিউটার, লগ, বা আনুষ্ঠানিক অন্যান্য যন্ত্রপাতি অধিগ্রহণ পদ্ধতি নির্ধারণ;

(চ) ভেন্ডর বা অন্য কোনো পক্ষের সহিত কার্য-সম্পাদন পদ্ধতি নির্ধারণ;

(ছ) ঘটনা পুনরাবৃত্তি প্রতিরোধের জন্য প্রশমন পদ্ধতি চিহ্নিতকরণ।

(২) প্রতেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উপ-অনুচ্ছেদ (১) এর অধীনে প্রণীত পরিকল্পনা সম্পর্কে উক্ত পরিকাঠামোর সহিত সংশ্লিষ্ট সকল ব্যক্তিকে উহার কার্যকরতা সম্পর্কে অবহিতক্রমে প্রয়োজনীয়তার নিরিখে উহা পর্যালোচনা ও মূল্যায়ন করিবে।

১২। সংকটকালীন (Crisis) যোগাযোগ:

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো, ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা প্রতিরোধের উদ্দেশ্যে, একটি সংকটকালীন যোগাযোগের ব্যবস্থার পরিকল্পনা প্রণয়ন করিবে, এবং উক্ত উদ্দেশ্যে গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) কোনো সংকটের সময় সহজে কার্যকর যোগাযোগ ব্যবস্থা গড়িয়া তুলিবার জন্য 'ক্রাইসিস ম্যানেজমেন্ট টিম' নামে একটি টিম গঠন করিবে;

(খ) সম্ভাব্য নিরাপত্তা বিঘ্নিত হইবার ঘটনার দৃশ্যকল্প চিহ্নিতকরণ ও উহা প্রতিরোধের ব্যবস্থা গ্রহণ করিবে;

(গ) উহার প্রতিনিধিত্বকারী ফোকাল পয়েন্ট মনোনীত করিবে;

(ঘ) গণমাধ্যমে এতদসংক্রান্ত তথ্য প্রচারের উদ্দেশ্যে যথাযথ প্লাটফরম বা চ্যানেল চিহ্নিত করিবে;

(ঙ) ক্ষতিগ্রস্থ পক্ষের সহিত দ্রুত ও কার্যকর যোগাযোগের উদ্যোগ প্রহণ করিবে;

(চ) উক্তরুপ পরিকল্পনা যথাযথভাবে কার্যকর করিবার উদ্দেশ্যে নিয়মিত অনুশীলনের ব্যবস্থা গ্রহণ করিবে।

অংশ-৭: পরিসম্পদ (Asset) ব্যবস্থাপনা

১৩। পরিসম্পদ ব্যবস্থাপনা:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর পরিসম্পদ চিহ্নিতকরণপূর্বক উক্ত পরিসম্পদের একটি তালিকা সমন্বয়ে একটি রেজিস্টার সংরক্ষণ করিবে।

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে ব্যবহৃত সম্মিলিত সিস্টেম (যেমন- হার্ডওয়্যার, সফটওয়্যার, নেটওয়ার্ক, ইত্যাদি) পরিসম্পদ অবশ্যই প্রযুক্তিগতভাবে হালনাগাদকৃত (updated) অবস্থায় থাকিতে হইবে। উক্ত তালিকায়, অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত বিষয়াদি অন্তর্ভুক্ত থাকিবে, যথা:-

(ক) পরিসম্পদের নামসহ উহার বিস্তারিত বিবরণ (উক্ত বিবরণে উৎপাদনকারী বা ভেন্ডর কর্তৃক এ পরিসম্পদটির রক্ষণাবেক্ষণের মেয়াদ লিপিবদ্ধ থাকিতে হইবে);

(খ) পরিসম্পদের গুরুত্বপূর্ণ কার্যাবলী;

(গ) উক্ত পরিসম্পদ ব্যবহারকারী অপারেটরের নাম;

(ঘ) পরিসম্পদের ভৌত বা ব্যবহারিক অবস্থান;

(ঙ) অভ্যন্তরীণ বা বহি:স্থ সিস্টেম বা নেটওয়ার্ক সহিত পরিসম্পদের নির্ভরশীলতার বিবরণ;

(চ) ভেন্ডর বা সরবরাহকারীর সহিত সম্পাদিত চুক্তির সংক্ষিপ্ত বিবরণ।

(৩) গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার নেটওয়ার্কের বহিঃপরিসীমা (perimeter) এবং উক্ত পরিকাঠামোর সহিত সংযুক্ত কম্পিউটার বা কম্পিউটার সিস্টেম শনাক্তক্রমে উহা উপ-অনুচ্ছেদ (১) এ বর্ণিত রেজিষ্টারে অন্তর্ভুক্ত করিবে।

(৪) এই অনুচ্ছেদে বর্ণিত রেজিষ্টারে অন্তর্ভুক্ত তালিকাভুক্ত পরিসম্পদ অনুচ্ছেদ ৮ এর অধীন ডিজিটাল নিরাপত্তা ঝুঁকি নিরূপণের আওতাভুক্ত হইবে।

অংশ-৮: গুরুত্বপূর্ণ তথ্য পরিকাঠামো সুরক্ষা সংক্রান্ত বিষয়াদি

১৪। মূল্যায়ন:

গুরুত্বপূর্ণ তথ্য পরিকাঠামোর মূল্যায়নের লক্ষ্যে এজেন্সি ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ এর বিধি ১২ অনুযায়ী প্রয়োজনীয় ব্যবস্থা গ্রহণ করিবে।

১৫। কম্পিউটার ইমার্জেন্সি রেসপন্স টিম গঠন:

ডিজিটাল নিরাপত্তা আইন, ২০১৮ ধারা ৯ এর উপ-ধারা (২) অনুযায়ী গুরুত্বপূর্ণ তথ্য পরিকাঠামো, প্রয়োজনে, ডিজিটাল নিরাপত্তা এজেন্সির পূর্বানুমোদন গ্রহণক্রমে, উহার নিজস্ব কম্পিউটার ইমার্জেন্সি রেসপন্স টিম গঠন করিতে পারিবে।

১৬। প্রবেশাধিকার নিয়ন্ত্রণ (Access Control):

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে উক্ত পরিকাঠামোর দায়িত্বপ্রাপ্ত কর্মচারীর অনুমোদিত প্রবেশাধিকার থাকিবে। ভেন্ডর বা অন্য কোনো ব্যক্তির উক্ত পরিকাঠামোতে প্রবেশ করিতে হইলে যথাযথ কর্তৃপক্ষের অনুমোদন থাকিতে হইবে। এইক্ষেত্রে তাহাদের প্রবেশাধিকার সীমিত ও নির্দিষ্ট সময়ের জন্য হইবে এবং দায়িত্বপ্রাপ্ত কর্মচারী কর্তৃক অনুমোদিত নয় এমন কোনো কর্মকান্ড পরিচালনা করা যাইবে না।

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ভৌত অবকাঠামোতে নিয়মিত প্রবেশকারী সকল ব্যক্তির কর্মচারী, ভেন্ডর, ইত্যাদি সরকারি বিধি-বিধান অনুযায়ী পুলিশ ভেরিফিকেশন বা সরকার কর্তৃক নির্ধারিত সংস্থা কর্তৃক নিরাপত্তা যাচাই করিতে হইবে।

অংশ-৯: ডিজিটাল নিরাপত্তা ব্যবস্থার নিরীক্ষা (Audit)

১৭। ডিজিটাল নিরাপত্তা ব্যবস্থা নিরীক্ষার বাধ্যবাধকতা:

(১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত কর্মচারী, মহাপরিচালক কর্তৃক নির্দেশিত সময়ের মধ্যে, স্বাধীনভাবে, তাহার নিয়ন্ত্রণাধীন পরিকাঠামোর ডিজিটাল নিরাপত্তার নিরীক্ষার ব্যবস্থা করিবে।

(২) উক্ত নিরীক্ষার মুখ্য উদ্দেশ্য হইবে, আইন, বিধিমালা ও এই গাইডলাইনের বিধান এবং মহাপরিচালক কর্তৃক, সময় সময়, জারীকৃত কর্ম-সম্পাদনের মানদণ্ড ও নির্দেশনা প্রতিপালিত হইতেছে কিনা উহা নিরূপণ করা।

(৩) উপ-অনুচ্ছেদে (১) এর অধীন নিরীক্ষা কার্য সম্পন্ন হইবার ৩০ (ত্রিশ) দিনের মধ্যে প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত কর্মচারী নিরীক্ষা প্রতিবেদনের অনুলিপি মহাপরিচালকের নিকট প্রেরণ করিবে।

(৪) উপ-অনুচ্ছেদ (১) এ যাহা কিছুই থাকুক না কেন, মহাপরিচালক, উক্ত উপ-অনুচ্ছেদের উদ্দেশ্য পূরণকল্পে, আদেশ দ্বারা, তৎকর্তৃক নিযুক্ত নিরীক্ষক দ্বারা কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে আইন, বিধিমালা ও এই গাইডলাইনের বিধান অনুসরণক্রমে নিরীক্ষা কার্য সম্পন্ন করিবার জন্য নির্দেশ দিতে পারিবেন।

(৫) উপ-অনুচ্ছেদ (৪) এর অধীন কোনো নির্দেশনা প্রদান করা হইলে, সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সংশ্লিষ্ট ব্যক্তি বা কর্মচারী নিরীক্ষা কার্য সম্পন্ন করিবার ব্যপারে নিরীক্ষককে পূর্ণ সহযোগিতা করিতে বাধ্য থাকিবে।

(৬) উপ-অনুচ্ছেদ (৩) এর অধীন সম্পন্নকৃত নিরীক্ষা ব্যয় সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো কর্তৃক নির্বাহ করিতে হইবে।

(৭) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরীক্ষা কার্যক্রম-

(ক) 'প্রথম শ্রেণী'র গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ক্ষেত্রে, মহাপরিচালক কর্তৃক নির্ধারিত কোনো প্রতিষ্ঠানের মাধ্যমে;

(খ) 'দ্বিতীয় শ্রেণী'র গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ক্ষেত্রে, সরকারি অথবা মহাপরিচালক কর্তৃক স্বীকৃত বেসরকারি প্রতিষ্ঠানের মাধ্যমে;

(গ) 'তৃতীয় শ্রেণী'র গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ক্ষেত্রে, মহাপরিচালক কর্তৃক স্বীকৃত বেসরকারি প্রতিষ্ঠানের মাধ্যমে,

সম্পন্ন করিতে হইবে।

(৮) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা ব্যবস্থা নিরীক্ষার সময়, নিরীক্ষক পরিশিষ্ট-৪ তে বর্ণিত দলিল পত্রাদির তালিকার (Document List) সহিত সমন্বয় করিয়া নিরীক্ষা কার্যক্রম সম্পন্ন করিবে।

১৮। সংশোধনী পরিকল্পনা:

(১) অনুচ্ছেদ ১৭ এর অধীন পরিচালিত নিরীক্ষায় যদি চিহ্নিত হয় যে, গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনায় এই গাইডলাইনের বিধান এবং মহাপরিচালক কর্তৃক জারিকৃত আদর্শ পরিচালন পদ্ধতি (SOP), কার্য-সম্পাদনের মানদণ্ড বা নির্দেশনা যথাযথভাবে প্রতিপালিত হইতেছে না, তাহা হইলে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত কর্মচারী নিরীক্ষা প্রতিবেদন প্রাপ্তির ৩০ (ত্রিশ) দিনের মধ্যে মহাপরিচালকের নিকট উক্ত পরিকাঠামো পরিচালনা সংক্রান্ত একটি সংশোধনী পরিকল্পনা উপস্থাপন করিবে।

(২) উক্ত পরিকল্পনায় কিভাবে নিরীক্ষায় চিহ্নিত করা বিষয়সমূহের প্রতিপালন যথাযথভাবে অনুসৃত হইবে উহার বিস্তারিত বিবরণসহ উহা উত্তরণের সময়সীমার উল্লেখ থাকিবে।

(৩) মহাপরিচালক, উক্ত পরিকাঠামোর কর্তৃপক্ষের সহিত আলোচনাক্রমে, প্রয়োজনে, তৎপ্রেক্ষিতে দাখিলকৃত সংশোধনী পরিকল্পনা পরিমার্জনক্রমে নূতন পরিকল্পনা দাখিলের জন্য নির্দেশ প্রদান করিতে পারিবেন, এবং উহা মহাপরিচালক কর্তৃক অনুমোদিত হইলে গুরুত্বপূর্ণ তথ্য পরিকাঠামো নিজ খরচে উক্ত পরিকল্পনা বাস্তবায়ন করিবে।

অংশ-১০: ডিজিটাল নিরাপত্তা সংক্রান্ত সচেতনতা সৃষ্টি

১৯। ডিজিটাল নিরাপত্তা ব্যবস্থা সম্পর্কে সচেতনতা সৃষ্টি:

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) উহার সকল কর্মচারী, ভেন্ডর ও উক্ত পরিকাঠামোতে প্রবেশাধিকার রহিয়াছে এমন সকল ব্যক্তির ডিজিটাল নিরাপত্তা ব্যবস্থা সম্পর্কে সচেতনতা সৃষ্টির জন্য প্রয়োজনীয় কর্মসূচী গ্রহণ করিবে; এবং

(খ) উক্ত কর্মসূচী উক্ত পরিকাঠামোর সহিত সংশ্লিষ্ট সকল শ্রেণীর কর্মচারী, ব্যবহারকারী, অপারেটর, ভেন্ডর ও সেবা প্রদানকারীর মধ্যে বহুল প্রচারের ব্যবস্থা গ্রহণসহ ডিজিটাল নিরাপত্তা সংক্রান্ত প্রযোজ্য আইন, বিধি, গাইডলাইন ও অন্যান্য বিধি-বিধানের প্রয়োগ সম্পর্কে সচেতনতা বৃদ্ধির প্রয়োজনীয় উদ্যোগ গ্রহণ করিবে।

২০। ডিজিটাল নিরাপত্তা ব্যবস্থা সম্পর্কে প্রশিক্ষণ:

গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনার দায়িত্বে নিয়োজিত প্রত্যেক কর্মচারীকে তথ্য প্রযুক্তি পরিচালনা সংক্রান্ত আন্তর্জাতিক প্রশিক্ষণ ও সনদ (যেমন- CCNA, CCNP, RHCE, MCSE, OCP, CompTIA, ITIL, ISO, ইত্যাদি), আইটি অডিট সংক্রান্ত প্রশিক্ষণ ও সনদ (যেমন- CISA, ISO Lead Auditor, ইত্যাদি), আইটি সিকিউরিটি সংক্রান্ত প্রশিক্ষণ ও সনদ (যেমন- CISSP, CISM, CRISC, OSCP, CEH, ইত্যাদি) অর্জন করিতে হইবে।

২১। ডিজিটাল নিরাপত্তা ব্যবস্থার অনুশীলন (Exercise):

(১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো ডিজিটাল নিরাপত্তা ব্যবস্থা সক্রিয় রাখার জন্য নিয়মিত অনুশীলন করিবে এবং জাতীয় পর্যায়ে আয়োজিত সাইবার ড্রিলে অংশগ্রহণ করিবে।

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনার দায়িত্বে নিয়োজিত কর্মচারী সাইবার আক্রমণ বিবেচনায় লইয়া সার্ভিস পুনরুদ্ধারের (Restore) বাস্তব ভিত্তিক বাৎসরিক পূর্ণাঙ্গ পরিকল্পনা অনুশীলন (Tabletop Exercise) করিবে।

(৩) উক্তরুপ অনুশীলন সংক্রান্ত কোনো তথ্য প্রদানের ব্যাপারে মহাপরিচালক কর্তৃক অনুরোধ প্রাপ্ত হইলে সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার ডিজিটাল নিরাপত্তা ব্যবস্থার অনুশীলন সংক্রান্ত তথ্যাদি মহাপরিচালকের নিকট প্রেরণ করিবে।

অংশ-১১: সরবরাহকারী ও সেবা প্রদানকারী ব্যবস্থাপনা

২২। সরবরাহকারী ও সেবা প্রদানকারী ব্যবস্থাপনা:

(১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার নিয়ন্ত্রণাধীন পরিকাঠামোতে প্রবেশ সংক্রান্ত তথ্য সংরক্ষণ, উক্ত পরিকাঠামোর সহিত যোগাযোগ এবং উক্ত পরিকাঠামো পরিচালনার সহিত সংশ্লিষ্ট ভেন্ডর বা সেবা প্রদানকারী কর্তৃক প্রদেয় সেবার জন্য সম্পাদিত তথ্য চুক্তিতে ডিজিটাল নিরাপত্তা ঝুঁকি প্রশমনের বিষয়ে প্রয়োজনীয় শর্ত আরোপ করিতে পারিবে।

(২) উক্ত চুক্তিতে, অন্যান্য বিষয়ের মধ্যে, নিরাপত্তা হুমকি প্রতিরোধের ক্ষেত্রে করণীয় বিষয়ের অন্তর্ভুক্ত থাকিবে।

(৩) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) ভেন্ডর বা সেবা প্রদানকারীর ডিজিটাল নিরাপত্তা ব্যবস্থার সহিত সংশ্লিষ্ট সকল পণ্যের বৈধতা প্রদান পদ্ধতি নির্ধারণ করিবে; এবং

(খ) আউট সোসিং এর মাধ্যমে উহার নিরাপত্তা ব্যবস্থা রক্ষণাবেক্ষণ করিতে পারিবে; তবে, আউট সোর্সিং এর মাধ্যমে নিযুক্ত সকল কর্মচারী, এবং উহার ভৌত অবকাঠামোতে নিয়মিত প্রবেশকারী সকল সরবরাহকারী ও সেবা প্রদানকারীর নিরাপত্তা যাচাই সরকারি বিধি-বিধান অনুযায়ী পুলিশ ভেরিফিকেশন বা সরকার কর্তৃক দায়িত্বপ্রাপ্ত সংস্থা দ্বারা সম্পন্ন করিতে হইবে।

অংশ ১২: নিরাপদ পরিচালন ব্যবস্থা

(এই অংশ কেবল অপারেশনাল প্রযুক্তি ব্যবস্থার ক্ষেত্রে প্রযোজ্য)

২৩। অপারেশনাল প্রযুক্তি:

(১) নেটওয়ার্ক বিভাজন (Network Segregation):

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) উহার নেটওয়ার্ক নকশাকে (Architecture) নেটওয়ার্ক জোনে বিভক্ত করিবে; এবং যেক্ষেত্রে উহার পরিচালনার জন্য কেবল কোনো একটি নেটওয়ার্ক জোনে কোনো তথ্য বা উপাত্ত প্রয়োজন হয়, সেইক্ষেত্রে উক্ত পরিকাঠামো হইতে অন্যান্য নেটওয়ার্ক জোনে উক্ত তথ্য বা উপাত্ত প্রেরণের জন্য উক্ত পরিকাঠামো হইতে যে নেটওয়ার্ক জোনে কোনো তথ্য বা উপাত্ত প্রেরণ করা হইবে সেই নেটওয়ার্ক জোনের মধ্যে যোগাযোগ সীমাবদ্ধ রাখিতে হইবে; এবং

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার বিভিন্ন জোনের মধ্যে অস্বাভাবিক তথ্য প্রবাহের নেটওয়ার্ক যোগাযোগ ব্যবস্থা পরিবীক্ষণ করিবে।

(২) প্রবেশাধিকার নিয়ন্ত্রণ (Access Restriction):

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-(ক) উহার আওতাধীন পরিকাঠামোতে দায়িত্ব ভিত্তিক প্রবেশাধিকার নিয়ন্ত্রণের ব্যবস্থাসহ উক্ত ব্যবস্থার সঠিক প্রয়োগ নিশ্চিত করিবার জন্য নিয়মিতভাবে পর্যালোচনা ও পরিবীক্ষণ করিবে।

(খ) পরিচালনার জন্য যৌথ ইউজার একাউন্টের প্রয়োজন হয়, সেইক্ষেত্রে উক্ত একাউন্টে অবৈধ অনুপ্রবেশ রোধ করিবার জন্য নিয়মিতভাবে একাউন্টসমূহের ব্যবহারিক প্রয়োগ পর্যালোচনা ও পরিবীক্ষণের জন্য যথাযথ পদ্ধতি অনুসরণ করিবে।

(গ) উহারব্যবহারিক কর্মকান্ড পর্যবেক্ষণের জন্য ইউজার একটিভিটি লগ রক্ষণাবেক্ষণ করাসহ অস্বাভাবিক কর্মকান্ড পর্যবেক্ষণের জন্য উক্ত লগ ব্যবস্থা নিয়মিতভাবে পুনঃনিরীক্ষণ করিবে; এবং

(ঘ) পরিসম্পদ ব্যবস্থাপনা সংক্রান্ত প্রিভিলেজড একাউন্টসমূহের জন্য বহুমুখী প্রমাণীকরণ (Multifactor Authentication) ব্যবস্থা গ্রহণ করিবে।

(৩) নেটওয়ার্ক এর নিরাপত্তা ব্যবস্থা:

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) উহার নেটওয়ার্ক এর জন্য অনুমোদিত নেটওয়ার্ক প্রটোকল চিহ্নিতক্রমে উহার বাস্তবায়ন প্রক্রিয়া অনুসরণের ব্যবস্থা গ্রহণক্রমে বিদ্যমান বেইজ লাইন পরিবর্তন ও নূতনভাবে নেটওয়ার্ক প্রটোকল সংযোজনের ক্ষেত্রে চেইঞ্জ ম্যানেজমেন্ট প্রসেস এর মাধ্যমে উহা বাস্তবায়িত করিবে; এবং

(খ) উহার নেটওয়ার্ক পরিচালনার ক্ষেত্রে সার্ভার ও কর্মক্ষেত্রে যথাযথ হোস্ট-ভিত্তিক নিরাপত্তার ব্যবস্থা গ্রহণ করিবে।

(৪) দূর নিয়ন্ত্রণ (Remote) সংযোগ ব্যবস্থা:

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার আওতাধীন পরিকাঠামোতে-

(ক) অবৈধ অনুপ্রবেশ প্রতিরোধ ও উহা শনাক্তের জন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সকল দূর নিয়ন্ত্রিত সংযোগ ব্যবস্থার কার্যকর ডিজিটাল নিরাপত্তা ব্যবস্থা গ্রহণ করিবে;

(খ) দূর নিয়ন্ত্রণ সংযোগের ক্ষেত্রে -

(অ) প্রয়োজনীয়তার নিরিখে, সম্ভাব্য ক্ষেত্রে, দূরবর্তী স্থান হইতে সংযোগ স্থাপন করিবে;

(আ) লভ্যতার (Avilable) ক্ষেত্রে, দৃঢ় প্রমাণীকরণ কৌশল (Authentication Technique), নিরাপত্তা সঞ্চালন (Transmission) ও মেসেজের শুদ্ধতা (Integrity) বাস্তবায়ন করিবে;

(ই) সকল নেটওয়ার্ক সংযোগের জন্য এনক্রিপশন বাস্তবায়ন করিবে;

(ঈ) ব্যবহারিক প্রয়োজনীয়তা না থাকিলে, গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে প্রভাবিত করিতে পারে এমন সিস্টেম কমান্ড হইতে দূর-নিয়ন্ত্রণ সংযোগ প্রদানে অসম্মতি জ্ঞাপন করিবে;

(উ) সংযোগের জন্য প্রয়োজনের অতিরিক্ত উপাত্তের প্রবাহ সীমাবদ্ধ করিবে ।

(৫) আক্রম্যতা (Vulnerabililty) নিরূপণ, ইত্যাদি:

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার পরিকাঠামোর নিরাপত্তা ও নিয়ন্ত্রণ ব্যবস্থার দুর্বলতা চিহ্নিতকরণের উদ্দেশ্যে মহাপরিচালক কর্তৃক নির্ধারিত সময়ের মধ্যে উহার আইটি বা ওটি (Operating Technology) সিস্টেমের দুর্বলতা নিরুপণের ব্যবস্থা করিবে; এক্ষেত্রে হোস্ট, অ্যাপ্লিকেশান ও নেটওয়ার্ক নিরাপত্তা ব্যবস্থা নিরূপণ এবং নিরাপত্তার নকশা পুনরীক্ষণসহ উহার আইটি সিস্টেমের পেনিট্রেশন টেস্ট সম্পন্ন করিতে হইবে;

(খ) উহার পরিকাঠামোতে অধিকতর গুরুত্বপূর্ণ নূতন আইটি সিস্টেম সংযোজন বা এপ্লিকেশন মডিউল, সিস্টেম আপগ্রেড বা প্রযুক্তিগত রিফ্রেশ পরিবর্তন বা সংযোজনের ক্ষেত্রে এবং চিহ্নিত আক্রম্যতা (Vulnerability) নিরূপণের জন্য দফা (ক) তে উল্লিখিত ব্যবস্থাদি গ্রহণ করিতে হইবে;

(গ) পেনিট্রেশন টেস্ট উহার প্রযুক্তিগত লভ্যতার ভিত্তিতে সম্পন্ন করাসহ কোনো তৃতীয় পক্ষের মাধ্যমে উক্ত টেস্ট করার ক্ষেত্রে পরিকাঠামোর সরাসরি তত্ত্বাবধানে সম্পন্ন করিবে;

(ঘ) মহাপরিচালক কর্তৃক নির্দেশিত হইলে প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো দুর্বলতা নিরূপণ ও পেনিট্রেশন টেস্ট এর ফলাফল অনতিবিলম্বে তাহার নিকট প্রেরণ করিবে।

(৬) এপ্লিকেশন এর নিরাপত্তা ব্যবস্থা:

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) উহাতে ব্যবহারের জন্য অনুমোদিত অ্যাপ্লিকেশান এর তালিকা প্রস্তুত করাসহ উক্ত তালিকায় কেবল উক্ত পরিকাঠামোর পরিচালনাগত ও ডিজিটাল নিরাপত্তা ব্যবস্থার প্রয়োজনীয় অ্যাপ্লিকেশান এর সংস্থান করিবে;

(খ) উহা পরিচালনা ও উহার ডিজিটাল নিরাপত্তা জন্য কেবল উক্তরুপ তালিকাভুক্ত এপ্লিকেশন ব্যবহার করিবে; এবং

(গ) যথাযথভাবে যাচাই প্রক্রিয়ার মাধ্যমে বৈধ উৎস হইতে অ্যাপ্লিকেশান ও প্যাচসমূহ সংগ্রহ ও উহা ব্যবহারের উপযোগী করিবে।

(৭) প্যাচ ব্যবস্থাপনা (Patch Management):

প্যাচ ব্যবস্থাপনার জন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামো নিম্নবর্ণিত ব্যবস্থাদি গ্রহণ করিবে, যথা:-

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামো জন্য যথাযথ প্যাচ ব্যবস্থাপনা থাকিতে হইবে, এবং উহাতে নিম্নবর্ণিত প্যাচ ব্যবস্থাপনার কৌশল থাকিতে হইবে-

(অ) পরিচালনা, দুর্বলতা, পরিবর্তন ও বাহ্যিক আকার (configuration) ব্যবস্থাপনা, ব্যাকআপ, পরীক্ষণ, নিরাপত্তা বিঘ্নিত হইবার ঘটনার রেসপন্স, বিপর্যয় পুনরুদ্ধার, ও অন্যান্য প্রক্রিয়ার সহিত প্যাচ ব্যবস্থাপনার সমন্বয়ের কৌশল প্রয়োগ করা;

(আ) পরিসম্পদের উপর প্রভাব পড়িতে পারে এমন সম্পদের প্যাচিং এর ক্ষেত্রে অগ্রাধিকার প্রদান করা;

(ই) পরিচালনার সময় আক্রম্যতা (Vulnerability) হ্রাসের জন্য সময়োচিত ও ধারাবাহিকভাবে কৌশলগতভাবে প্যাচ প্রয়োগ করা;

(ঈ) উপরি-বর্ণিত ব্যবস্থাদি গ্রহণ করা কারিগরিভাবে সম্ভাপর না হইলে অন্য কোন সমতুল্য ব্যবস্থা গ্রহণ করা;

(খ) উক্তরুপ প্যাচ গুরুত্বপূর্ণ পরিকাঠামোর কার্মকান্ড বা ডিজিটাল নিরাপত্তা ব্যবস্থা অনিচ্ছাকৃতবাবে ব্যাহত হইয়াছে কিনা উহা নির্ণয়ের জন্য উক্ত পরিকাঠামোর বিদ্যমান পরিবেশ অক্ষুন্ন রাখিয়া সকল প্যাচ এর পরীক্ষা সম্পন্ন করিতে হইবে।

(৮) পরিবীক্ষণ ও শনাক্তকরণ (Observation and Identification):

প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে উহার লগ সংক্রান্ত সকল ঘটনার জন্য উক্ত পরিকাঠামো একটি কনসিসটেন্ট টাইম সোর্স ব্যবহার, উহার স্বভাবিক পরিচালনার জন্য উক্ত পরিকাঠামোর প্রত্যাশিত নেটওয়ার্ক প্রবাহ ও কার্য-সম্পাদন প্রক্রিয়ার ভিত্তিরেখা প্রস্তুত এবং ডিজিটাল নিরাপত্তা ব্যবস্থার হুমকি নিয়ন্ত্রণে দৃষ্টিগ্রাহ্য নিয়ন্ত্রণ এবং উক্তরুপ নিরাপত্তা ব্যবস্থার ধারাবাহিক পরিবীক্ষণের ব্যবস্থা গ্রহণ করিতে হইবে।

অংশ-১৩: বিবিধ

২৪। নির্দেশ প্রদানের ক্ষমতা:

কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামো এই গাইডলাইন প্রতিপালনে অসমর্থ হইলে, মহাপরিচালক, লিখিতভাবে, উক্তরূপ কারণ সম্বলিত ব্যাখ্যা চাহিয়া এই গাইডলাইন অনুসরণের জন্য নির্দেশ প্রদান করিতে পারিবে; এবং উক্তরূপে কোনো নির্দেশ প্রদান করা হইলে সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহা প্রতিপালনে বাধ্য থাকিবে।

২৫। অব্যাহতি:

মহাপরিচালক, কোনো বিশেষ পরিস্থিতি পরিহারের উদ্দেশ্যে, কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোর আবেদনের পরিপ্রেক্ষিতে, কোনো নির্দিষ্ট সময়ের জন্য, এই গাইডলাইনের সুনির্দ্দিষ্ট কোনো বিধানের প্রয়োগ হইতে, মহাপরিচালক কর্তৃক আরোপিত শর্ত সাপেক্ষে, অব্যাহতি প্রদান করিতে পারিবে।

২৬। গাইডলাইনের সীমাবদ্ধতা:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামো স্ব স্ব ক্ষেত্রে (Domain) সাইবার সিকিউরিটি, আইসিটি নীতিমালা, পরিকল্পনা ও বাস্তব ভিত্তিক অতিরিক্ত সুরক্ষা পদ্ধতি এবং বাস্তবায়ন করিতে হইবে। উক্ত ক্ষেত্রে এই গাইডলাইন গুরুত্বপূর্ণ তথ্য পরিকাঠামোর জন্য একটি সহায়ক নির্দেশিকা হিসেবে বিবেচিত হইবে।

(২) এই গাইডলাইন এর অন্যতম লক্ষ্য হইবে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ন্যূনতম সুরক্ষার নির্দেশনা বাস্তবায়ন করিবার জন্য সাংগঠনিকভাবে প্রাথমিক সরঞ্জাম (Tools) এবং পন্থা (Approaches) সম্পর্কে নির্দেশনা প্রদান করা।

(৩) প্রযুক্তিগত পরিবর্তন, বিভিন্ন মাধ্যম হতে প্রাপ্ত জ্ঞান, বাস্তব অভিজ্ঞতার ভিত্তিতে এই গাইডলাইন নিয়মিতভাবে হালনাগাদ করা যাইবে।

পরিশিষ্ট-১: অনুসরণীয় উত্তম চর্চা (Best Practices)

(অংশ ৩, অনুচ্ছেদ (৪)(১)(ঞ) দ্রষ্টব্য)

গুরুত্বপূর্ণ তথ্য পরিকাঠামোসমূহ উহার নিরাপত্তা ব্যবস্থা সুরক্ষার ক্ষেত্রে নিম্নবর্ণিত উত্তম চর্চা অনুসরণ করিবে, যথা:-

(ক) পরিকল্পনার মাধ্যমে নিয়ন্ত্রণ:

(১) পরিকল্পনা বিষয়ক:

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কৌশলগত পরিকল্পনার সহিত সংগতিপূর্ণ তথ্য নিরাপত্তার লক্ষ্য ও উদ্দেশ্য অর্জনের জন্য বাৎসরিক কর্ম পরিকল্পনা প্রণয়ন এবং উহার সীমা সুনির্দ্দিষ্ট করাসহ উহা বাস্তবায়ন করা;

(খ) আইনগত ও নিয়ন্ত্রণমূলক ব্যবস্থাদি অনুধাবন করা;

(গ) তথ্য নিরাপত্তার কর্ম পরিকল্পনার ব্যবস্থাপনা, রক্ষণাবেক্ষণ, ইত্যাদির জন্য প্রয়োজনীয় অর্থের সংস্থান করা;

(ঘ) ISO/IEC ২৭০০১ মান বা স্ট্যান্ডার্ড অনুসরণে তথ্য নিরাপত্তা ব্যবস্থাপনার সিস্টেমের নিরাপত্তা ঝুঁকি ব্যবস্থাপনার কাঠামো নির্ধারণ।

(২) উন্নয়ন বিষয়ক:

(ক) তথ্য নিরাপত্তার ব্যবস্থা উন্নয়নে যথাযথ নীতি, মানদণ্ড, গাইডলাইন ও পদ্ধতি নির্ধারণ করা;

(খ) তথ্য নিরাপত্তা ব্যবস্থার দলিলাদি প্রণয়ন, উহা পর্যালোচনা, হালনাগাদ ও আনুষ্ঠানিকভাবে বাস্তবায়ন করা;

(গ) তথ্য ও পরিসম্পদ শ্রেণীকরণ নীতি-কাঠামো প্রণয়ন;

(ঘ) উপরোক্ত দফা (অ), (আ) ও (ই) তে বর্ণিত কার্যাদি সম্পাদনে সংশ্লিষ্ট অংশীজনের পরামর্শ গ্রহণ করা।

(৩) ব্যবস্থাপনা বিষয়ক:

(ক) তথ্য নিরাপত্তার নীতি, পদ্ধতি ও এই গাইডলাইনে বিধৃত নীতি-নির্দেশনার বহুল প্রচারের ব্যবস্থা করা;

(খ) নিরাপত্তা ঝুঁকি নিরূপণ ও নিরাপত্তা বিঘ্নিত হওয়ার ঘটনা নিয়ন্ত্রণের ব্যবস্থা গ্রহণ করা, এবং তথ্য নিরাপত্তা সম্পর্কে সচেতনতা বৃদ্ধির উদ্দেশ্যে উক্ত বিষয়ে অভ্যন্তরীণ ও বহি:স্থ রিপোর্টিং করা;

(গ) নিরাপত্তা বিষয়ে সচেতনতা বৃদ্ধিতে সম্পৃক্ত হওয়াসহ যথাযথ প্রশিক্ষণের ব্যবস্থা করা;

(ঘ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কর্ম-সম্পাদন (Business) প্রক্রিয়ার সহিত তথ্য নিরাপত্তা ব্যবস্থা সংহত (Integration) করা;

(ঙ) তথ্য নিরাপত্তা ব্যবস্থার নীতি, মানদন্ড, পদ্ধতি, ইত্যাদির কার্যকরতার মূল্যায়ন ও পর্য্যালোচনা করা;

(চ) তথ্য নিরাপত্তা বিঘ্নিত হইবার ঘটনাসমূহের বিবরণের রেকর্ড সংরক্ষণ করা;

(ছ) তথ্য নিরাপত্তা ব্যবস্থার নির্দেশিকার জন্য পরিসম্পদ ব্যবস্থাপনার নীতি অন্তর্ভুক্ত করাসহ গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রবেশ ও নিগর্মন ব্যবস্থাপনার কৌশল নির্ধারণ করা;

(জ) নিরাপদ ইলেকট্রনিক বর্জ্য ব্যবস্থাপনা নিশ্চিত করা;

(ঝ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর আওতাধীন সকল তথ্য ব্যবস্থা যথাযথভাবে রক্ষণাবেক্ষণ ও হালনাগাদ করা।

(৪) পর্যবেক্ষণ বিষয়ক:

(ক) বিদ্যমান তথ্য নিরাপত্তা পরিচালন পদ্ধতির (Security Operational Process) কার্যকরতা মূল্যায়ন করা;

(খ) তথ্য নিরাপত্তা সংক্রান্ত আইনগত ও নিয়ন্ত্রণমূলক নীতির যথাযথ প্রতিপালন মূল্যায়ন করা;

(গ) তথ্য নিরাপত্তা ব্যবস্থার নিরীক্ষা কার্য সম্পাদন করা;

(ঘ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা উহার তথ্য প্রযুক্তি ব্যবস্থার কোনরূপ পরিবর্তনের ক্ষেত্রে সার্বক্ষণিক (২৪*৭*৩৬৫ দিন) ভিত্তিতে কার্য-সম্পাদন করা।

খ) ব্যবস্থাপনার মাধ্যমে নিয়ন্ত্রণ:

(১) পরিসম্পদ ব্যবস্থাপনা ও উহার তালিকা প্রস্তুতকরণ:

(ক) পরিসম্পদ ও উহার তালিকা ব্যবস্থাপনার জন্য, প্রতিপালনীয় দায়িত্ব অর্পণক্রমে, একটি বিশেষ টিম নিয়োজিত করা;

(খ) প্রত্যেক হার্ডওয়্যার ডিভাইস (যেমন- সার্ভার, প্রিন্টার, ল্যাপটপ, ডেস্কটপ, এক্সেস ডিভাইস, অগ্নিনির্বাপন সংক্রান্ত যন্ত্রপাতি, ইত্যাদি) ক্রমিক নম্বর সহযোগে সুস্পষ্টভাবে চিহ্নিত করা;

(গ) সফটওয়্যার এর নাম, উহার সংস্করণ, সিরিয়াল নম্বর, যে ডিভাইসের সহিত উহা সংযোজন করা হইয়াছে উহার তালিকা প্রস্তুতক্রমে নিয়মিতভাবে হালনাগাদ করা;

(ঘ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সংবেদনশীল স্থানে কোনো যন্ত্রপাতি, ডিজিটাল মিডিয়া, ইত্যাদির ভৌত অবস্থান পরিবর্তন বা স্থানান্তরের ক্ষেত্রে যথাযথ নিয়ন্ত্রণমূলক ব্যবস্থা গ্রহণ করা;

(ঙ) ব্যবস্থাপনা কর্তৃপক্ষের অনুমোদন ব্যতীত কোন পরিসম্পদ পরিবর্তন, বিক্রয় বা বাতিল না করা এবং উক্তরূপে কোন পরিবর্তন, বিক্রয় বা বাতিল করা হইলে সম্পদের তালিকা যথাযথভাবে হালনাগাদ করা;

(চ) পরিসম্পদ ও উহার তালিকা নিয়মিতভাবে নিরীক্ষা করা এবং তথ্য ও যোগাযোগ প্রযুক্তি সম্পর্কিত ডিভাইসসমূহ যাচাই করা;

(ছ) তথ্য ও পরিসম্পদ শ্রেণীকরণ তালিকা যথাযথভাবে হালনাগাদ করা।

(২) প্রবেশাধিকার নিয়ন্ত্রণ:

(ক) বৈরী পরিস্থিতি মোকাবেলার জন্য, একক দায়িত্বের পরিবর্তে, কর্মরত ব্যক্তি বা কর্মচারীগণের দায়িত্ব পৃথক করা;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নীতির আলোকে 'আবশ্যকতার ভিত্তিতে' কর্মরত কর্মচারী বা ব্যক্তির দায়িত্ব অর্পণ করা;

(গ) সিস্টেমে প্রবেশের ক্ষেত্রে উহার ব্যবহার ও ধরনের ভিত্তিতে গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রয়োজনীয়তার নিরিখে প্রবেশাধিকার চিহ্নিত করা;

(ঘ) ভূমিকা ও দায়িত্বের ভিত্তিতে কর্মরত ব্যক্তি বা কর্মচারী চিহ্নিতক্রমে ক্ষমতা অর্পন করা;

(ঙ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রবেশ ও নির্গমনের ক্ষেত্রে প্রবেশাধিকার নীতির পরিপূর্ণ বাস্তবায়ন করা;

(চ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কার্য-সম্পাদনের দায়িত্ব পালনের সূত্রে যথাযথ ইউজার একাউন্ট প্রস্তুত বা খোলার মাধ্যমে কম্পিউটারে সিস্টেমে প্রবেশ নিয়ন্ত্রণের কার্যকর ব্যবস্থা গ্রহণ করা;

(ছ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নেটওয়ার্কে প্রবেশ নিয়ন্ত্রণ সংক্রান্ত ব্যবস্থা নিয়মিতভাবে যাচাই করা;

(জ) প্রবেশ নিয়ন্ত্রণ নীতিমালা বাস্তবায়ন প্রক্রিয়া পরিবীক্ষণ এবং উহার বাস্তবায়ন লঙ্ঘন বা ব্যত্যয় সংক্রান্ত বিষয়াদির গতিবিধি পর্যবেক্ষণ ও নিয়ন্ত্রণ করা;

(ঝ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর প্রয়োজনীয়তার নিরিখে নিয়মিতভাবে নিরীক্ষা কার্য সম্পন্ন করা;

(ঞ) ডিভাইস কনফিগারেশন এ যৌক্তিক প্রবেশ কেবল এডমিনিসট্রেটরের মধ্যে সীমাবদ্ধ রাখা।

(৩) শনাক্তকরণ ও প্রমাণীকরণ (Authentication) নিয়ন্ত্রণ:

(ক) যথাযথ শনাক্তকরণ নীতি বাস্তবায়ন করা; এইক্ষেত্রে কোনো কাজ করিবার অনুমতি প্রদানের পূর্বে সকল ব্যবহারকারীকে অনন্যভাবে চিহ্নিত করা;

(খ) শনাক্তকরণ ও প্রমাণীকরণের মাধ্যমে গুরুত্বপূর্ণ তথ্য পরিকাঠামো সহিত সম্পৃক্ত নয় এমন ব্যক্তির প্রবেশাধিকার নিয়ন্ত্রণ ব্যবস্থা পর্যালোচনা করা; এবং উক্ত পরিকাঠামোর চাকুরি হইতে বরখাস্তকৃত বা চাকুরি পরিত্যাগকারী কর্মচারীর প্রবেশাধিকার নিয়ন্ত্রণ করা;

(গ) নিরাপদ পদ্ধতিতে পাসওয়ার্ড সংরক্ষণ করা;

(ঘ) কার্য-সম্পাদনের বিষয়াদি বিবেচনাক্রমে প্রমাণীকরণ নীতির বাস্তবায়ন করা যাহাতে ব্যবহারকারী কর্তৃক সম্পাদনকৃত সকল কর্মকান্ড চিহ্নিত করা যায়;

(ঙ) ব্যবহারকারীর ক্ষতিগ্রস্থ বা চুরি যাওয়া পরিচয় ও পাসওয়ার্ড অক্ষম (Disable) করার পদ্ধতি নির্ধারণ করা;

(চ) ব্যবহারকারীর বারবার ব্যর্থ প্রচেষ্টার উপর আবশ্যিকভাবে যুক্তিসংগত বিধি-নিষেধ আরোপ করা;

(ছ) ব্যবহারকারীর একাউন্টস ও প্রবেশাধিকার নিয়ন্ত্রণের কার্যকর পরিবীক্ষণ ব্যবস্থা গ্রহণ করা;

(জ) উক্ত বিষয়ে যথাযথ নিরীক্ষা কার্য সম্পন্ন করাসহ উক্ত বিষয়ে সংশ্লিষ্ট সকলের মতামতের ভিত্তিতে নিয়ন্ত্রণ ব্যবস্থা জোরদার করা এবং উহার বাস্তবায়ন কৌশল নির্ধারণ করা ।

(৪) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর বহি:পরিসীমা (Perimeter) সুরক্ষা:

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর বহি:পরিসীমা সুরক্ষার জন্য পরিকল্পনা প্রণয়ন ও উহার বাস্তবায়ন করা;

(খ) অবাঞ্চিত প্রবেশ শনাক্তকরণে প্রয়োজনীয় শনাক্তকরণ ও সুরক্ষা ব্যবস্থার প্রয়োগ নিশ্চিত করা;

(গ) যথাযথ প্রবেশ নিয়ন্ত্রণ তালিকা (Access Control List) সহযোগে সকল অর্ন্তমূখী ও বর্হিমূখী সংযোগ ব্লক করার ব্যবস্থা করা;

(ঘ) প্রায়োগিকভাবে যথাযথ সুরক্ষা নীতি সহযোগে ফায়ারওয়াল ব্যবহার করা; এইক্ষেত্রে অর্ন্তমূখী ও বর্হিমূখী তথ্য প্রবাহের ওয়েব কনটেন্ট ফিল্টার এর ব্যবস্থা করা;

(ঙ) স্পুফকৃত ই-মেইল ব্লক করার জন্য ‘সেন্ডার নীতি-কাঠামো’ এর কৌশল নির্ধারণ করা;

(চ) “আইপি এড্রেস” এর পরিবর্তে ডোমেইন এর মাধ্যমে ওয়েবসাইটে প্রবেশের অনুমতি প্রদানের ব্যবস্থা করা;

(ছ) সকল প্রবেশপথে (Gateway) ব্যবহৃত এন্টি-ভইরাস ও এন্টিম্যালওয়্যার সর্বদা হালনাগাদকরণ করা;

(জ) নিরাপত্তা ব্যবস্থার পরিকাঠামোর সংবেদনশীল পরিবর্তনের ক্ষেত্রে ‘চেইঞ্জ ম্যানেজমেন্ট প্রসেস’ এর সহিত সংগতিপূর্ণ করা;

(ঝ) বহি:পরিসীমা জোনের আওতাধীন সকল ডিভাইসে প্রবেশাধিকার নিয়ন্ত্রণ, প্রমাণীকরণ এবং অডিটিং লগিং ব্যবস্থা কর্যকর করা;

(ঞ) অভ্যন্তরীণ পরিকাঠামোর অংশ বিশেষের সিস্টেম, এপ্লিকেশন, ও ডাটাবেইজের নিরাপত্তা নিশ্চিত করা;

(ট) সার্ভার, ই-মেইল সার্ভার, বা প্রমাণীকৃত ওয়েব প্রক্সির মাধ্যমে ইন্টারনেট সেবা গ্রহণের বিষয়টি পরিবীক্ষণ ও নিরীক্ষার আওতাভুক্ত করা;

(ঠ) আগম্যমান (Incoming) সংযোগ ট্র্যকিং এর জন্য প্রক্সির মাধ্যমে প্রবেশের ক্ষেত্রে ওয়েব সার্ভারকে অনুমোদন প্রদান করা।

(৫) ভৌত (Physical) অবকাঠামোগত ও পরিবেশগত (Environmental) নিরাপত্তা:

(ক) ভৌত অবকাঠামোগত নিরাপত্তা নিয়ন্ত্রণ ব্যবস্থার যথাযথ পরিকল্পনা গ্রহণ করা;

(খ) প্রাকৃতিক ও ভৌত অবকাঠামোগত ঝুঁকি মোকাবেলার জন্য দুর্যোগ ব্যবস্থাপনা বা পুনরূদ্ধার পরিকল্পনা গ্রহণ করা;

(গ) পরিবেশগত ঝুঁকির কারণে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরাপত্তার জন্য যথাযথ জলবায়ুগত ও নির্ভুল নিয়ন্ত্রণ ব্যবস্থা গ্রহণ করা, এবং উক্ত পরিকাঠামোর কার্যালয় স্থির বিদ্যুৎতের নেতিবাচক প্রভাব হইতে যথাযথ সুরক্ষার ব্যবস্থা গ্রহণ করা;

(ঘ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে অনুমোদিত ব্যক্তির প্রবেশ রোধ করিবার জন্য যথাযথ নিরাপত্তা ব্যবস্থা গড়িয়া তোলাসহ পর্যাপ্ত সংখ্যক নিরাপত্তা কর্মী নিয়োজিত করা;

(ঙ) ভৌত অবকাঠামোগত ঝুঁকি মোকাবেলার জন্য প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার কর্মচারীগণ দ্বারা, সময় সময়, মক ড্রিল (Mock drill) এর ব্যবস্থা গ্রহণ করাসহ উহা নিয়মিতভাবে উহা নিরীক্ষা করা;

(চ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে নিয়োজিত কর্মচারীগণের সৌহার্দপূর্ণ সম্পর্ক স্থাপনসহ পারস্পারিক সন্দেহজনক ব্যবহার পরিবীক্ষণ করা;

(ছ) ভৌত অবকাঠামোর নিরাপত্তা ব্যবস্থার ফাঁকফোকর বন্ধের ব্যবস্থা গ্রহণ করা;

(জ) কেবল অনুমোদিত ব্যক্তির প্রবেশ নিশ্চিত করিবার লক্ষ্যে প্রবেশ নিয়ন্ত্রণ কৌশল গড়িয়া তোলা।

(৬) হার্ডওয়্যার ও সফটওয়্যার এর পরীক্ষা মূল্যায়ন:

(ক) হার্ডওয়্যার ও সফটওয়্যার এর ক্রয়ের ক্ষেত্রে যথাযথ বিধি-বিধান অনুসরণ ও ব্যবহারের ক্ষেত্রে মূল্যায়নের মানদণ্ড নির্ধারণ করা;

(খ) সময় উপযোগী যন্ত্রপাতি ও সফটওয়্যার স্থাপনের পূর্বে পরীক্ষা ও মূল্যায়ন করা এবং তদুদ্দেশ্যে চেকলিষ্ট প্রস্তুত করা;

(গ) হার্ডওয়্যার ও সফটওয়্যার এর হালনাগাদ ও প্যাচিং চিহ্নিত করা; এইক্ষেত্রে যতদূর সম্ভব অচল ও সেকেলে প্রযুক্তির ব্যবহার পরিহার করা;

(ঘ) মানসম্পন্ন হার্ডওয়্যার ও সফটওয়্যার ব্যবহার করা।

(গ) পরিচালনাগত নিয়ন্ত্রণ:

(১) উপাত্ত সংরক্ষণ: হ্যাশিং ও এনক্রিপশন:

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সংবেদনশীল উপাত্ত সংরক্ষণের জন্য যথাযথ হ্যাশিং ও এনক্রিপশন সম্পর্কিত নীতি-নির্দেশনার যথাযথ বাস্তবায়ন করা;

(খ) ব্যাকআপ উপাত্তসহ সংরক্ষিত উপাত্তের হ্যাশিং ও এনক্রিপশন সম্পর্কিত নিদের্শনার যথাযথ বাস্তবায়ন করা;

(গ) উপাত্তের হ্যাশিং ও এনক্রিপশন সংক্রান্ত নির্দেশনার লঙ্ঘন প্রতিহত করা;

(ঘ) নিয়মিতভাবে হ্যাশিং ও এনক্রিপশন এর জন্য বাস্তবায়িত এ্যালগোরিদম এর শক্তিমত্তা পরীক্ষা ব্যবস্থার মূল্যায়ন করা; এবং ইতিমধ্যে বাস্তবায়িত এ্যালগোরিদমে যদি কোনরূপ সমস্যা দেখা দেয়, তাহা হইলে উপাত্তের হ্যাশিং এ এনক্রিপশনের জন্য নূতন এ্যালগোরিদমের বাস্তবায়ন প্রবর্তন করা।

ব্যখ্যা।- এনক্রিপশন হইল এমন একটি প্রক্রিয়া যাহাতে প্রযুক্তি দ্বারা গাণিতিক অ্যালগরিদমের সহায়তায় প্লেইনটেক্স উপাত্ত বা ডাটাকে এনকোড করিয়া সাইফারটেক্স ডেটাতে রূপান্তর করা হইয়া থাকে। অভীষ্ট প্রাপক প্রযুক্তি ব্যবহারের মাধ্যমে (Intended Recipient) উক্ত সাইফারটেক্সকে ডিকোড করিয়া প্লেইনটেক্স উপাত্তে রূপান্তর করিতে পারিবে। এইক্ষেত্রে এনক্রিপশনের অন্যতম মূল উদ্দেশ্য হইতেছে উপাত্ত বা ডাটা এর গোপনীয়তা (Confidentiality) বজায় রাখা। আবার হ্যাশিং এর মূল উদ্দেশ্য হইতেছে উপাত্ত বা ডাটা এর শুদ্ধতা (Integrity) বজায় রাখা।

(২) নিরাপত্তা বিঘ্নিত হইবার ঘটনা ব্যবস্থাপনা:

(ক) নিরাপত্তা বিঘ্নিত হওয়ার ঘটনা প্রতিরোধের জন্য পরিকল্পনা গ্রহণক্রমে উক্ত বিষয়ে সংশিষ্ট সকলের দায়িত্ব নির্ধারণ এবং উক্ত পরিকল্পনায় সুস্পষ্টভাবে এসকেলেশন মেট্রিক্স সীমা অন্তর্ভুক্ত করা;

(খ) নিরাপত্তা বিঘ্নিত হইবার ঘটনা ঘটিবার সময় নিয়োজিত কর্মচারীগণের কর্তব্য ও সিদ্ধান্ত গ্রহণ প্রক্রিয়া ব্যবস্থাপনা করা;

(গ) নিরাপত্তা বিঘ্নিত হইবার ঘটনা নিয়ন্ত্রণ ও পুনরুদ্ধার পরিকল্পনা সংশ্লিষ্ট সকলকে অবহিত করা;

(ঘ) সিস্টেম সক্রিয় করিবার পূর্বে পুনরুদ্ধার এবং অরক্ষিত অবস্থা অপসারণের ব্যবস্থা নিশ্চিত করা; এবং একবার পুনরুদ্ধার করা হইলে, নিরাপত্তা ব্যবস্থা বিঘ্নিত হইবার ঘটনা ও অবাঞ্চিত প্রবেশের চিহ্ন মুছিয়া ফেলা ও উহা বিশ্লেষণ করা;

(ঙ) ভবিষ্যত নিরাপত্তা বিঘ্নিত হইবার ঘটনা প্রতিরোধের উদ্দেশ্যে উক্তরুপ ঘটনা বিশ্লেষণের পর এতদবিষয়ের সুপারিশসমূহ ব্যবস্থাপনা কর্তৃপক্ষের নিকট উপস্থাপন করা।

(৩) দক্ষতা উন্নয়ন, প্রশিক্ষণ, ইত্যদি:

(ক) প্রশিক্ষণের কৌশল, পরিকল্পনা ও কর্মসূচী পর্যালোচনা করা;

(খ) অরক্ষিত অবস্থা ও নিরাপত্তা ঝুঁকি চিহ্নিতকরণ ও মূল্যায়ন করা;

(গ) দক্ষতা উন্নয়ন কর্মসূচী ও প্রশিক্ষণ ব্যবস্থার মূল্যায়ন করা;

(ঘ) দক্ষতা উন্নয়নের প্রয়োজনীয়তা নিরূপন ও উহা বাস্তবায়ন করা;

(ঙ) দক্ষতা উন্নয়ন কৌশল এবং সহযোগী প্রক্রিয়া বা পদ্ধতি সম্পর্কে গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে নিয়োজিত কর্মচারীদের শিক্ষা, প্রশিক্ষণ প্রদানের ব্যাপারে প্রশিক্ষণ কাঠামো প্রস্তুত করা।

(৪) উপাত্তের (Data) ক্ষতি প্রতিরোধ:

(ক) সকল ধরনের উপাত্ত সংরক্ষণ ডিভাইস চিহ্নিত ও শনাক্ত করা ও উহাদের বৈধতা প্রদান করা;

(খ) বিভিন্ন ধরনের উপাত্ত সংরক্ষণের জন্য মজুদের তালিকা বিন্যস্ত করা; এবং উহা সংরক্ষণের জন্য ব্যাকআপ পরিকল্পনা করা;

(গ) ট্র্যাকিং এর মাধ্যমে অননুমোদিত উপাত্ত প্রবাহ পরিবীক্ষণের জন্য নেটওয়ার্ক মনিটরিং টুলস ব্যবহার করা;

(ঘ) কনটেন্ট ফিল্টারিং পেরিমিটার প্রটেকশন ডিভাইস দ্বারা নিয়ন্ত্রিত ও শ্রেণীবিন্যস্ত তথ্য ব্লক করা; এইক্ষেত্রে কনটেন্ট-এওয়্যার, ডীপ প্যাকেট ইন্সপেকশন, ই-মেইল ও অন্যান্য প্রটোকল ব্যবহার করা;

(ঙ) মোবাইল স্টোরেজ ডিভাইস (যেমন- ইউএসবি, সিডি, স্মার্ট ফোন, ইত্যাদি) এর ব্যবস্থাপনা ও ব্যবহার নিয়ন্ত্রণের জন্য একক তথ্য নিরাপত্তা নীতি গ্রহণ করা;

(চ) স্টোরেজ ডিভাইসের উপাত্তের সুরক্ষার জন্য যথাযথ এনক্রিপশন এলগোরিদম ব্যবহার করা;

(ছ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিয়ম নীতি অনুসরণে সুনির্দিস্ট কনটেন্ট এর ব্যবহার শনাক্ত ও ব্লক করা বা নিয়ন্ত্রণের মাধ্যমে তথ্য ফাসের চেষ্টা নিয়ন্ত্রণ করা;

(জ) উপাত্তের ক্ষয়ক্ষতি রোধের জন্য যথাযথ ভারসাম্যমূলক ব্যবস্থা গ্রহণ করা;

(ঝ) ভৌত ও পরিবেশগত নিরাপত্তামূলক ব্যবস্থা গ্রহণসহ শ্রেণীবিন্যস্ত উপাত্তে অবৈধ অনুপ্রবেশ শনাক্তের ব্যবস্থা করা;

(ঞ) অফিসিয়াল যোগাযোগ ও চিঠিপত্র আদান প্রদানের ক্ষেত্রে অফিসিয়াল ই-মেইল আইডি ব্যবহার করা এবং প্রযোজ্য ক্ষেত্রে ডিজিটাল স্বাক্ষর ও এনক্রিপশন ব্যবহার করা;

(ট) প্রান্তবিন্দু (end point) সুরক্ষা ব্যবস্থার মাধ্যমে কর্মক্ষেত্রের কম্পিউটার নিয়ন্ত্রণ করা।

(৫) পেনিট্রেশন টেস্টিং:

(ক) ডিজিটাল নিরাপত্তার সকল স্তর সুরক্ষার বিষয় বিবেচনায় লইয়া (যেমন- ভৌত, অভ্যন্তরীণ, বহিঃস্থ, নেটওয়ার্ক, পেরিমিটার সুরক্ষা, হার্ড ওয়্যার, সফট ওয়্যার, উপাত্ত সুরক্ষা প্রবেশাধিকার নিয়ন্ত্রণ, ইত্যাদি) পেনিট্রেশন টেস্ট সম্পন্ন করা;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিজস্ব কর্মচারী বা এতদবিষয়ক অভিজ্ঞ ব্যক্তি বা প্রতিষ্ঠানের মাধ্যমে উহার সম্পদের পেনিট্রেশন টেস্ট সম্পাদনের কর্ম-পদ্ধতির কৌশল নির্ধারণ করা;

(গ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিজস্ব কর্মচারী ব্যতীত বহিঃস্থ কোনো ব্যক্তি বা প্রতিষ্ঠানের মাধ্যমে পেনিট্রেশন টেস্ট সম্পাদনের ক্ষেত্রে উক্ত ব্যক্তি বা প্রতিষ্ঠানের সহিত নন-ডিসক্লোজার চুক্তি (Non Disclosure Agreement) সম্পাদন করিতে হইবে যাহাতে পেনিট্রেশন টেস্ট সম্পাদনের সময় সংগৃহীত সংরক্ষিত তথ্য কোনোভাবেই ফাঁস না হইয়া যায়;

(ঘ) পেনিট্রেশন টেস্ট সম্পাদনের সময় কোনক্রমেই গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কোনরূপ পরিচালনাগত ক্ষতি করা যাইবে না তাহা নিশ্চিত করা;

(ঙ) পেনিট্রেশন টেস্ট সম্পাদনের ক্ষেত্রে সময়ে আক্রম্যতা (Vulnerability) পরীক্ষার সময় সিস্টেম যাহাতে বন্ধ না হইয়া যায় সেই দিকে সতর্ক দৃষ্টি রাখা এবং ইহা বিস্তৃত পরিসরে ও সুচিন্তিতভাবে সম্পন্ন করা;

(চ) রিয়েল টাইম টেস্ট করা সম্ভবপর না হইলে সেইক্ষেত্রে ডিজিটাল নিরাপত্তা এজেন্সি কর্তৃক নির্ধারিত পদ্ধতিতে পেনিট্রেশন টেস্ট সম্পাদন করা;

(ছ) পেনিট্রেশন টেস্ট এর ফলাফলের ভিত্তিতে উহা পর্যালোচনাপূর্বক বাস্তবায়ন করা।

(৬) নেটওয়ার্ক ডিভাইস সুরক্ষা:

(ক) বলিষ্ঠ (Strong) পাসওয়ার্ড ব্যবহার করা;
(খ) নির্দ্দিষ্ট সময় অন্তর পাসওয়ার্ড পরিবর্তন করা;
(গ) নিরাপত্তা ব্যবস্থার নীতি অনুসরণে প্রবেশাধিকার নিয়ন্ত্রণ করা;
(ঘ) অন্তর্মূখী ও বর্হিমূখী তথ্য প্রবাহ পরিবীক্ষণ ও বিশ্লেষণ করা;
(ঙ) নিরাপত্তা ব্যবস্থার সহিত সামঞ্জস্যহীন অংশ হালনাগাদ করা;
(চ) নেটওয়ার্ক টপোলজি (Topology) ও আর্কিটেকচার সমন্বয় করা।

(৭) গুরুত্বপূর্ণ বা সংবেদনশীল তথ্যের স্টোরেজ মিডিয়া হস্তান্তর (Disposal) ও স্থানান্তর (Transfer):

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ব্যবস্থাপনা কর্তৃপক্ষ কর্তৃক নির্ধারিত কারিগরি ও প্রশাসনিক গাইডলাইনের ভিত্তিতে উহার সকল তথ্যের স্টোরেজ মিডিয়া হস্তান্তর ও স্থানান্তরের ব্যবস্থাসহ উহা নিয়মিতভাবে নিরীক্ষার ব্যবস্থা করা;

(খ) উক্তরূপে তথ্যের স্টোরেজ মিডিয়া হস্তান্তর ও স্থানান্তরের যথাযথ লগ সংরক্ষণ করাসহ উহা যথাযথ রেজিস্টারে অন্তর্ভুক্ত করা;

(গ) ফেরত পাওয়া মিডিয়া স্টোরেজ অগ্নি-নিরোধক আধারে নিরাপদভাবে সংরক্ষণের ব্যবস্থা করাসহ উহা যথাযথ রেজিস্টারে অন্তর্ভুক্ত করা;

(ঘ) যাহাতে প্রয়োজনীয় তথ্য নষ্ট বা হারাইয়া না যায় সেইজন্য যথাযথ সতর্কতার সহিত গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ক্লিন ডেস্ক পলিসি (Clean Desk Policy) বাস্তবায়ন করা।

(৮) ইন্ট্রানেট এর নিরাপত্তা ব্যবস্থাপনা:

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর তথ্য নিরাপত্তা ব্যবস্থাপনার নীতির আলোকে ইন্ট্রানেট এর নিরাপত্তার ব্যবস্থা করা;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে উহার পরিচালনাগত পদ্ধতির আলোকে ইন্ট্রানেট এ প্রবেশের ধরন (যেমন- এমপ্লয়ী একসেস, রেসট্রিকটেড ইউজার একসেস, রেসট্রিকটেড উইজার এডিটিং একসেস, এডমিনেসট্রেটিভ একসেস, ইত্যাদি) নিয়ন্ত্রণের ব্যবস্থা করা, এবং উক্ত ক্ষেত্রে বায়োমেট্রিক্স, স্মাটকার্ড, পাসওয়ার্ড, ইত্যাদি ব্যবহার করা;

(গ) ইন্ট্রানেট এ তথ্য নিবেদিত করার ক্ষেত্রে আবশ্যিকভাবে উহা এনক্রিপটেড ও পাসওয়ার্ডের সুরক্ষা প্রদান করা, এবং ব্যবহারকারী শ্রেণী বিভাজনের ভিত্তিতে কেবল অনুমোদিত ব্যবহারকারীকে কোনো ফাইল দেখা ও সম্পাদনের অনুমতি প্রদান করা;

(ঘ) পাবলিক নেটওয়ার্ক হইতে ইন্ট্রানেট যথাসম্ভব বিচ্ছিন্ন রাখা;

(ঙ) সর্বশেষ সংস্করণের প্যাচ, এন্টিভাইরাস, অপারেশন কন্ট্রোল, এটি-ম্যালওয়্যার, নিরাপদ স্বাক্ষর, ইত্যাদির মাধ্যমে ইন্ট্রানেট এর সকল সিস্টেম নিয়মিতভাবে হালনাগাদ করা;

(চ) ইন্ট্রানেট এ তথ্য সঞ্চালন প্রবাহ ব্যবস্থা সম্পূর্ণরূপে লগিং করা এবং উহা নিয়মিতভাবে পরিবীক্ষণ করা;

(ছ) নির্দিষ্ট সময় অন্তর ইন্ট্রানেট নেটওয়ার্ক নিরীক্ষা করা;

(জ) পেনড্রাইভ, হার্ডওয়্যার ডিভাইস, ইত্যাদির ব্যবহার নিষিদ্ধ করা বা প্রয়োজনীয় যাচায়ের পর উহা ব্যবহারের অনুমতি প্রদান করা, এবং অনুরূপ কোনো ব্যবহার নিয়মিতভাবে পরিবীক্ষণ করা;

(ঝ) ক্ষতিকর তথ্য প্রবাহ (যেমন- স্প্যাম, ফিশিং, স্পাইওয়্যার, অ্যাডওয়্যার, ম্যালওয়্যার, ইত্যাদি) ব্লক বা ট্র্যাক করিবার জন্য ইন্ট্রানেট এ ই-মেইল ফিল্টার রাখা;

(ঞ) ইন্ট্রানেট এ রক্ষিত গোপনীয় তথ্য ব্যবস্থায় ক্ষতিকর হামলাকারীর অননুমোদিত প্রবেশ রোধ করিবার জন্য ট্রান্সপোর্ট লেয়ার সিকিউরিটি (TLS) ডিজিটাল সনদের ব্যবহার করা।

(৯) পুন: পুন: হামলার ঘটনার সুরক্ষা:

(ক) ইন্টারনেট এর মাধ্যমে অপরিহার্যভাবে তথ্য প্রেরণের ক্ষেত্রে, সর্বোচ্চ নিরাপত্তা ও গোপনীয়তা অবলম্বন করা যায় এমন উন্নত ধরনের প্রযুক্তি ব্যবহার করা;

(খ) ইলেকট্রানিক তথ্য প্রেরণের ক্ষেত্রে, অবশ্যই পাসওয়ার্ড দ্বারা সুরিক্ষত ও বহুমাত্রিক (Multiple) ইলেকট্রনিক প্রতিবন্ধক দ্বারা নিরাপত্তা ব্যবস্থা সংরক্ষিত করা;

(গ) কম্পিউটার একাউন্টে প্রবেশের অনুমতি প্রদানের একটি গুরুত্বপূর্ণ বিষয়। এইক্ষেত্রে সিস্টেম এ্যাডমিনিসট্রেটর ও ব্যবহারকরীগণকে প্রবেশের সীমিত অধিকার প্রদান করা;

(ঘ) ম্যালওয়্যার আক্রমণ হইতে সুরক্ষা পাইবার জন্য নিয়মিতভাবে সকল ধরনের কম্পিউটার সিস্টেম সফটওয়্যার, সিকিউরিটি প্যাচ ও অন্যান্য প্রয়োজনীয় সুরক্ষা ব্যবস্থা হালনাগাদ করা;

(ঙ) পুন: পুন: হামলার ঘটনা সম্ভাব্য দ্রুততার সহিত সংশ্লিষ্ট কর্তৃপক্ষকে অবহিত করিতে হইবে এবং এইক্ষেত্রে উক্তরুপ হামলার সময়, তারিখ, হামলার ঘটনার ধরন ও উহার প্রতিরোধ পদ্ধতি, প্রভাব, ইত্যাদি তথ্য উক্ত কর্তৃপক্ষকে প্রদান করা।

(১০) উপাত্ত ব্যাক-আপ ও উহার পুনরুদ্ধার পরিকল্পনা:

(ক) উপাত্ত ব্যাকআপ নির্বাচন করিবার সময় গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ব্যবসায়িক প্রয়োজন ও রেগুলেটরি বাধ্যবাধকতা পরখ করিয়া সেই চাহিদা অনুযায়ী ব্যাকআপের ডাটা রিটেনশান নির্বাচন করা;

(খ) উপাত্ত ব্যাকআপ নিয়মিত পরখ করা, যে ব্যাকআপ যথাযথভাবে সম্পন্ন করা হইয়াছে সেই ব্যাকআপের কোনো ব্যত্যয় ঘটিলে তাহা সংশ্লিষ্ট কর্তৃপক্ষকে অবহিত করা;

(গ) ব্যাকআপ হইতে উপাত্ত পুনরুদ্ধার (Restore) করা যায় কিনা তাহা পরখ করা এবং এই প্রক্রিয়াটি মূল সার্ভারে সম্পন্ন না করা;

(ঘ) উপাত্ত পুনরুদ্ধার (Restore) টেস্টের জন্য পৃথক একটি টেস্ট সার্ভার ব্যবহার করা। পুনরুদ্ধার টেস্ট করিবার পর টেস্ট সংক্রান্ত দলিল সংরক্ষণ করিতে হইবে এবং উহাতে নিম্নলিখিত তথ্যাবলি সন্নিবেশিত করিতে হইবে যাহাতে পরবর্তীতে আদর্শ পরিচালনা পদ্ধতি (Standard Operating Procedure) হিসেবে গণ্য করা যায়: -

(অ) উপাত্ত পুনরুদ্ধার করিবার সময়;

(আ) পুনরুদ্ধারকৃত ডাটার পরিমান;

(ই) পুনরুদ্ধার করিবার সংশ্লিষ্ট প্রকৌশলীর নাম;

(ঈ) পুনরুদ্ধার করিবার প্রক্রিয়া, ইত্যাদি;

(ঙ) আকস্মিক দুর্ঘটনা সংঘটিত হইবার পর উহা পুনরুদ্ধারের জন্য বিকল্প স্থান নির্বাচন সংক্রান্ত আনুষ্ঠানিক নীতি পদ্ধতি নির্ধারণ ও উহার বাস্তবায়ন করা;

(চ) বিকল্প স্থান নির্বাচনের পূর্বে ভৌত-কাঠামোর ও পরিবেশগত হুমকির বিষয়ে যথাযথ সাবধানতা অবলম্বন করা;

(ছ) বিকল্প স্থান হইতে কার্য-সম্পাদনের ক্ষেত্রে, অর্থ বরাদ্ধসহ দায়িত্ব পালন সংক্রান্ত বিষয়াদি সুনির্দিষ্টভাবে নিরুপণ করা;

(জ) বিকল্প স্থান নির্ধারণের ক্ষেত্রে, বিদ্যুৎ, পানি, যোগাযোগের ব্যবস্থা, ইন্টারনেট সংযোগ ব্যবস্থা, ইত্যাদির মৌলিক সুযোগ-সুবিধা যাচাই করা;

(ঝ) আকস্মিক দুর্ঘটনার সময় পরিচালনাগত করনীয় ব্যবস্থা সম্পর্কে প্রশিক্ষণ ও সরেজমিন অনুশীলনের মাধ্যমে গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে নিয়োজিত কর্মচারীসহ সংশ্লিষ্ট সকলকে সচেতন করা;

(ঞ) আকস্মিক দুর্ঘটনার ফলে বিকল্প স্থানে স্বাভাবিকভাবে কার্য-সম্পাদনের প্রয়োজনে সংবেদনশীল উপাত্তের ব্যাক আপ রাখা।

(১১) নিরাপদ ও সহিষ্ণু নকশা (Resilient Architecture) বিস্তারণ:

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কার্য-সম্পাদন ও প্রয়োজনীয়তার নিরিখে উহার তথ্য নিরাপত্তার ক্ষেত্রে, নিরাপদ ও সহিষ্ণু নকশা বিস্তারণের পরিকল্পনা করা;

(খ) নেটওয়ার্ক নকশায় নিরাপত্তার ব্যবস্থাকে একটি গুরুত্বপূর্ণ উপাদান হিসেবে সংযুক্ত করা;

(গ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর তথ্য নিরাপত্তা ব্যবস্থার সহিত সমন্বয়পূর্বক তথ্য ও যোগাযোগ প্রযুক্তি ব্যবস্থার সামগ্রিক নকশা প্রণয়ন করা;

(ঘ) নিরাপত্তা ও ব্যবসায়ের মধ্যে ভারসাম্যপূর্ণ নকশা নির্বাচন করা;

(ঙ) তথ্য নিরাপত্তার বিষয়টি বিবেচনাক্রমে, নকশা বিস্তারণের পূর্বে পণ্যের অটোমেশন, ইন্ডাসট্রিয়াল নিয়ন্ত্রণ ও আবেক্ষণিক (Supervisory) নিয়ন্ত্রণ ও উপাত্ত অধিগ্রহণের পরীক্ষণ মূল্যায়ন করা;

(চ) নিরাপত্তা ব্যবস্থার নকশা বিস্তারণের আওতায় তথ্য ও যোগাযোগ প্রযুক্তি ব্যবস্থা ও উহার যন্তপাতি সুদৃঢ়ভাবে স্থাপন করা;

(ছ) অটোমেটেড আপগ্রেডস ও লগ মনিটরিং ব্যবস্থা নিরাপত্তা ব্যবস্থার নকশা বিস্তারণের অংশ করা;

(জ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরাপত্তা ব্যবস্থার নকশা প্রণয়ণের ক্ষেত্রে, অভ্যন্তরীণ নেটওয়ার্ক, ভার্চুয়াল লোকাল এরিয়া নেটওয়ার্ক, ইন্ট্রানেট রক্ষণাবেক্ষণ, দূর নিয়ন্ত্রণ সেবার ব্যবস্থা, পেরিমিটার সুরক্ষা যন্ত্রপাতি ও নিরাপত্তা প্রদান সংক্রান্ত যন্ত্রপাতি হইতে মিলিটারাইজড ডোমেইন ও ডি-মিলিটারাইজড জোন যথাযথভাবে পৃথক করা;

(ঝ) দ্রুত পরিবর্তনশীল তথ্য প্রযুক্তির নিরাপত্তা ব্যবস্থার সহিত খাপ খাওয়াইয়া নিরাপত্তা ব্যবস্থার নকশা হালনাগাদ করিবার ব্যবস্থা করা;

(ঞ) সংবেদনশীল যোগাযোগের ব্যবস্থা ও উহার যোগাযোগের চ্যানেলসমূহ সুরক্ষার ব্যবস্থা করা, যাহাতে সিকিউরড সকেট লেয়্যার বা অন্য কোন পদ্ধতিতে আড়িপাতা সংক্রান্ত বিষয়াদি পরিহার করা যায়।

(১২) নিরাপত্তা ব্যবস্থার হুমকি সংক্রান্ত বিষয়ের রিপোর্টিং:

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামো ও এজেন্সির মধ্যে দ্বিমূখী ফিডব্যাক ব্যবস্থাপনার অংশীদারিত্ব গড়িয়া তুলিবার জন্য যথাযথ পদ্ধতি উদ্ভাবন করা;

(খ) এজেন্সির নিকট হইতে, সময় সময়, প্রাপ্ত গোপনীয় তথ্যাদি এবং গুরুত্বপূর্ণ তথ্য পরিকাঠামো হতে প্রাপ্ত গোপনীয় তথ্যাদি যাহাতে প্রকাশ না পায় সেইজন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামো ও এজেন্সির মধ্যে পারস্পরিক নন-ডিসক্লোজার চুক্তি সম্পাদন করা;

(গ) এজেন্সির কর্তক, সময় সময়, আয়োজিত কর্মশালা, সেমিনার প্রশিক্ষণ কর্মসূচীতে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কর্মচারীদের অংশগ্রহণের ব্যবস্থা করা;

(ঘ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে নিরাপত্তা ব্যবস্থার হুমকির ঘটনা ও অবাঞ্ছিত প্রবেশের ক্ষেত্রে যাহাতে সরকারী সংস্থার তথ্যের নিরাপত্তা যাহতে বিঘ্নিত না হয় সেইজন্য প্রয়োজনীয় ব্যবস্থা গ্রহণ করা;

(ঙ) সাইবার ড্রিল, পেনিট্রেশন টেস্টিং সংক্রান্ত পরামর্শ বাস্তবায়ন সংক্রান্ত তথ্য যথাবিহিতভাবে এজেন্সিকে অবহিত করা; এবং উক্তরুপ গুরুত্বপূর্ণ তথ্য সম্পর্কে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ফিডব্যাক চ্যানেলের মাধ্যমে এজেন্সিকে রিপোর্ট করা;

(চ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো কর্তৃক নিরাপত্তা ব্যবস্থা সম্পর্কিত বিষয়ে প্রয়োজনীয় প্রশিক্ষণ, কর্মশালা, ইত্যাদি আয়োজন ব্যবস্থা করা।

(১৩) নিরীক্ষা এবং আক্রম্যতা (Vulnerability) নিরুপণ:

(ক) ডিজিটাল নিরাপত্তা ব্যবস্থা নিরুপণ ও উহার নিরীক্ষার ব্যবস্থা গ্রহণ করা;

(খ) দুর্বলতা নিরুপণ ও উহা নিরীক্ষার অনুসূচী প্রণয়নের পূর্বে নিরাপত্তা ব্যবস্থার হুমকি চিহ্নিতকরণ ও অগ্রাধিকার নির্ণয়ে সমন্বিত অনুশীলন করা;

(গ) দুর্বলতা বিষয়ে প্রশিক্ষণ প্রদান, সচেতনতা বৃদ্ধি, নিরীক্ষা, ইত্যাদির মাধ্যমে ডিজিটাল নিরাপত্তা ব্যবস্থার প্রায়োগিক ব্যবস্থা গ্রহণ করা;

(ঘ) নিরীক্ষা কার্যে তথ্য ব্যবস্থা ও লগ ডকুমেন্টের পদ্ধতি অন্তর্ভুক্ত করা;

(ঙ) সংবেদনশীল সেবা ও তথ্য ব্যবস্থাপনার সহিত সম্পর্কিত সকল যন্ত্রপাতি, ডিভাইস ও সফটওয়্যার এর নিরীক্ষা ও দুর্বলতা নিরুপণ নীতি প্রয়োগ করা এবং উক্তরুপ নীতির লঙ্ঘন ডিজিটাল নিরুপণ ব্যবস্থা লঙ্ঘন ও শাস্তিযোগ্য বলিয়া বিবেচনা করা।

(১৪) ডিজিটাল নিরাপত্তা সংক্রান্ত সুপারিশ বাস্তবায়ন:

(ক) সম্ভাব্য সকল ঝুঁকি ব্যবস্থাপনার (Manage Risk) জন্য একটি সুষ্ঠ ও নিয়মতান্ত্রিক প্রক্রিয়ার মাধ্যমে প্রতিষ্ঠানের সুরক্ষা নীতি অনুমোদন ও কৌশল বাস্তবায়নের জন্য প্রয়োজনীয় বাজেট বরাদ্দ, দায়িত্ব বণ্টন এবং মূল্যায়ন করা;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে ডিজিটাল নিরাপত্তা ব্যবস্থা সংক্রান্ত সুপারিশ বাস্তবায়নের জন্য তথ্য নিরাপত্তা গভর্ন্যান্স কমিটি, তথ্য নিরাপত্তা স্টিয়ারিং কমিটি (Information Security Steering Committee) এবং কমপ্লায়েন্স কমিটি গঠন করা;

(গ) ডিজিটাল নিরাপত্তা ব্যবস্থা সংক্রান্ত সুপারিশ বাস্তবায়নের বিষয়ে রিপোর্ট প্রনয়ণের জন্য কৌশল প্রণয়ন করা;

(ঘ) ডিজিটাল নিরাপত্তা ব্যবস্তার সুপারিশ ব্যবস্থাপনা পর্যালোচনা ও পরিবীক্ষণ করা;

(ঙ) ডিজিটাল নিরাপত্তা ব্যবস্থার সুপারিশ বাস্তবায়িত না হওয়ার ক্ষেত্রে প্রয়োজনীয় অনুসন্ধান বা তদন্তের ব্যবস্থা করা;

(চ) ডিজিটাল নিরাপত্তা ব্যবস্থার সুপারিশ গুরুত্বপূর্ণ তথ্য পরিকাঠামোর তথ্য নিরাপত্তা নীতির অংশ করা;

(ছ) বিধি-বিধান লঙ্ঘন বিষয়ে তাৎক্ষণিকভাবে রিপোর্ট প্রদানক্রমে উক্ত বিষয়ে যথাযথ ব্যবস্থা গ্রহণ করা।

(১৫) তথ্য নিরাপত্তা গভর্ন্যান্স (Information Security Governance):

তথ্য নিরাপত্তা গভর্ন্যান্স একটি সার্বিক ব্যবস্থাপনা কাঠামো যাহা প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর উদ্দেশ্য এবং কার্যক্রমকে সমন্বয়সাধন করে। এইক্ষেত্রে সংশ্লিষ্ট সকলকে গুরুত্বপূর্ণ তথ্য পরিকাঠামো কর্তৃক প্রণীত তথ্য সুরক্ষা নীতি মানিয়া চলিতে হইবে এবং অভ্যন্তরীণ নিয়ন্ত্রণের (Internal Controls) মাধ্যমে প্রযোজ্য বিধি-বিধান বাস্তবায়ন করিতে হইবে।

পরিশিষ্ট- ২: তথ্য প্রেরণ ছক

(অংশ-৪, অনুচ্ছেদ ৬(৪) দ্রষ্টব্য)

PROVIDING INFORMATION TO AGENCY

Information relating to Critical Information Infrastructure (CII)	
The owner of the Critical information infrastructure is required to provide the following information to the Agency-	
A. The following information on the design, configuration and security of the critical information infrastructure:	
i. A network diagram depicting every key component and interconnection in the critical information infrastructure, and any external connection and dependency that the critical information infrastructure may have	
ii. For every key component in the critical information infrastructure, the following details*: (Fill the box in the right side of the below table)*	
a) Its name and description;	
b) Its physical location;	
c) Any operating system and version;	
d) Any key software and version;	

	e) Its internet protocol address and any open port, if the component is internet facing;		
	f) The name and address of the owner		
	g) The name and address of the operator		

iii. The types of data processed on or stored in the critical information infrastructure *(Fill in the box below)*

iv. The name and contact of every individual having overall responsibility for the cybersecurity of the critical information infrastructure;

Name	Contact	Job role

B. The following information on the design, configuration and security of any other computer or computer system under the owner's control that is interconnected with or that communicates with the critical information infrastructure *(Fill the box in the right side of the below table)*		
	i. The name and description of that other computer or computer system;	
	ii. The physical location of that other computer or computer system;	
	iii. The name and address of its operator, if the owner is not the operator;	

	iv.	A description of any function provided by that other computer or computer system;	
	v.	The types of data exchanged with the critical information infrastructure;	
	vi.	The operating system and version;	
	vii.	The key software and version;	

viii.	How that other computer or computer system is interconnected with or communicates with the critical information infrastructure, including the communication protocol of that other computer or computer system with the critical information infrastructure;	

C. The name of any outsourced service provider supporting the critical information infrastructure, and the nature of the outsourced service; and such other information as the Agency may require in order to ascertain the level of cybersecurity of the critical information infrastructure. (Fill in the box below)

Official Stamp of CII

Singature and Date

পরিশিষ্ট-৩ক: প্রাথমিক মূল্যায়ন ফরম

(অংশ-৫, অনুচ্ছেদ ৭ (২) দ্রষ্টব্য)

(Initial Assessment Form)

Track Number/Reference Number:

Name of Critical information infrastructure:
(Fill in the box below)

Focal point of contact for Critical information infrastructure:
(Fill in the box below)

Name	
Designation	
E-mail:	
Phone Number	
Postal Address	

Secondary point of contact for Critical information infrastructure:
(Fill in the box below)

Name	
Designation	
E-mail:	
Phone Number	
Postal Address	

Information Security Event Description

Description of the Event

Provide brief summary:

Service Impacts in CIA Triad

Confidentiality	Integrity	Availability

Business Impacts in brief summary

Vulnerabilities Identified

Provide brief summary:

Information Security Event Details

Description	Date	Time
Event occurred		
Event discovered		
Event reported		

Is the Event Over? ☐ Yes ☐ No

POC	Official Stamp of CII

Agency Will fill up

Agency Receiving Person Name & Designation

Receiving Time & Date

Agency Official Stamp

পরিশিষ্ট -৩খ: চূড়ান্ত মূল্যায়ন ফরম

(অংশ-৫, অনুচ্ছেদ ৭ (৩) দ্রষ্টব্য)

(Final Assessment Form)

Track Number/Reference Number:

Name of Critical information infrastructure:
(Fill in the box below)

Focal point of contact for Critical information infrastructure:
(Fill in the box below)

Name	
Designation	
E-mail:	
Phone Number	
Postal Address	

Secondary point of contact for Critical information infrastructure:
(Fill in the box below)

Name	
Designation	
E-mail:	
Phone Number	
Postal Address	

Information Security Event Description

Description of the Event:

What Occurred

- ☐ Loss of service Loss of equipment Loss of facility
- ☐ System malfunction System overload
- ☐ Software malfunction Intrusion attempt
- ☐ Human error
- ☐ Bad application design
- ☐ Compliance violations Access violations Physical/security breach Uncontrolled system changes Others (please specify)

How Occurred

- ☐ Theft Fraud
- ☐ Sabotage/Physical Damage
- ☐ Malicious Code
- ☐ Hacking/Logical Infiltration
- ☐ Misuse of Resources Hardware Failure
- ☐ Software Failure
- ☐ Hardware Maintenance Error
- ☐ Communication Failure
- ☐ Fire
- ☐ Flood Design
- ☐ Error User
- ☐ Error
- ☐ Operations Error
- ☐ Software Maintenance Error
- ☐ Third Party Services
- Others (please specify)_____

Why Occurred

- ☐ Deliberate or Intentional
- ☐ Actual Attack Accidental
- ☐ Others _____

Description of the Event in details: (Provide as much as information for understand the incident)

Related Business Impacts

- ☐ Financial Loss
- ☐ Personal Information
- ☐ Legal and Regulatory
- ☐ Obligations
- ☐ Disruption to Business Operations
- ☐ Vulnerabilities Identified: (Provide as much as information for understand the Vulnerability)

Others (please specify)_____

Information Security Event Details

Description	Date	Time
Event occurred		
Event discovered		
Event reported		

Is the Event Over? ☐ Yes ☐ No

Provide brief summary of associate events:

S

POC	Official Stamp of CII

TYPE OF INFORMATION SECURITY INCIDENT

☐ Actual ☐ Attempted ☐ Suspected

Threat Source Occurred at what Level

☐ Organizational ☐ Level Process ☐ Level Information System Level

Type of Threat Event ☐ Adversarial ☐ Non Adversarial

Assets Affected

(Provide descriptions of the assets affected by or related to the incident including serial, license, version numbers where relevant)

Information/Data .....

Hardware .....

Software .....

Communications .....

Documentation .....

Business Impact/Effect of Incident

(Provide descriptions of the assets affected by or related to the incident including serial, license, version numbers where relevant)

		Value
Breach of Confidentiality	☐	.....
Breach of Integrity	☐	.....
Breach of Availability	☐	.....
Breach of Non-Repudiation	☐	.....
Destruction	☐	.....

Additional Notes:

INCIDENT RESOLUTION

Incident Investigation Commenced Date .....

Incident Investigator(s) Name(s) .....

Incident End Date .....

Impact End Date .....

Incident Investigation Completion Date .....

Reference and Location of Investigation Report .....

Actions Taken to Resolve Incident

Actions Taken to Resolve Incident	

Actions Outstanding

Actions Outstanding (Investigation is still required by other personnel)	

Current Status of Incident

Current Status of Incident (Open/unresolve/resolve/close/Need Escalation)	

CONCLUSION

Identified Root Cause	**Recommendation for Improvement**

পরিশিষ্ট-৪: প্রামান্য দলিল পত্রাদির তালিকা

(অংশ ৯, অনুচ্ছেদ ১৭ (৮) দ্রষ্টব্য)

Internal Information Security Policies and Processes

SL No.	Document Name (Applicable Based on Business and Operations)
Policy and Process	
1	Information Security Policy
2	Acceptable Use policy
3	Asset and Data Management Policy
4	Communication Security Policy
5	Compliance Policy
6	Human Resource Security Policy
7	Information Security Continuity Policy
8	Information Security Incident Management Policy
9	Cryptography Policy
10	Log Management Policy
11	Logical Access Control Policy
12	Mobile Device, Teleworking and BYOD Policy
13	Operation Security Policy
14	Physical and Environmental Security Policy
15	Availability Management Process
16	Business Relationship Management Process
17	Capacity Management Process
18	Change Management Process

SL No.	Document Name (Applicable Based on Business and Operations)
19	Configuration Management Process
20	Continual Service Improvement Process
21	Documentation Management Process
22	Incident and Service Request Management Process
23	Internal IT Audit Process
24	Release and Deployment Management Process
25	Service Continuity Management Process
26	Service Level Management Policy
27	Cloud Service Policy
28	IT Asset and Data Management Policy
29	Problem Management Process
30	Information Security Steering Committee Formation Policy
31	Data Backup and Restore policy
32	Asset Disposal Policy
Human Resource (HR) Documents	
1	Approved organogram
2	Job Description (Roles and Responsibility Matrix)
3	Background verification from LEA (NSI, SB and DGFI)
4	Employee training related to IT Security
Data Center operations related Documents	
1	Floorplan of Data Center
2	Camera layout and related documents
3	Substation and Generator Health Related Report
4	Network topology diagram
5	Data Center Maintenance Report
6	Server Rack layout Diagram
7	Top of the rack switch diagram
8	Vendor Agreement (SLA, AMC and OMC)

SL No.	Document Name (Applicable Based on Business and Operations)
9	Data Backup Drill
10	Operating System patch and update details
11	Approved Software List
12	Service/System Availability Report
Capacity related documents	
1	Data Storage capacity Report
2	Public IP block usage
3	Power consumption
4	Bandwidth consumption
5	HVAC capacity and usage
6	Server Capacity and Health Check Report
7	Network Capacity and Health Check Report
8	IT and Security Incident Monitoring Report
9	Data Backup Daily Report
Standard Operating Procedure (SOP)	
1	Data Center SOP
2	SOP for all application and database
3	SOP for other related IT Operations
NDA, SLA, Services and Forms related documents	
1	Service Catalogue
2	Non-Disclosure Agreement (NDA)
3	Service Level Agreement (SLA) and Customer related forms
4	User access form and process diagram
5	Change management form
Supporting Documents	
1	Supporting document for Penetration Testing and/or vulnerability scanning
2	Supporting document for Remote Access with/without 2-factor authentication

SL No.	Document Name (Applicable Based on Business and Operations)
3	Supporting Document for Disaster Recovery and Business continuity Planning
4	Supporting document for log (Audit logs, transaction logs, event logs, error logs, message logs etc.) management
5	Approved IT Risk Register and Risk Treatment
6	Previous Internal/External IT Audit Report
7	Gap Analysis Report (Based on ISO 27001)
8	Access Control and Privilege User Control List
9	Classification of Information and Asset
Inventory	
1	IT Warehouse visiting report
2	Approved Software List used in the organization
3	Standard Software details of NOC PC/Laptops and MDC
4	Software licensing details
5	Operating System Licenses details
6	IT Asset List
Other Documents and Reports	
1	Fire-drill report
2	Service Request, Incident & Change Documents
3	Root Cause Analysis (RCA)
4	Other Relevant Documents

পরিশিষ্ট-৫: ঝুঁকি রেজিস্টার

(অংশ-৫, অনুচ্ছেদ ৮ (১) দ্রষ্টব্য)

(Risk Register)

Risk ID	Risk Enlisting Date	Information Security Objective (s) Affected (confidentiality/ integrity /availability)	Affected Asset	Risk description	Linked/Consequence Risk	Vulnerability	Threat	Likelihood	Impact	Risk Ratings (VeryLow/ Low/Medium/ High/Very High)	Priority	Risk Owner	Risk Treatment			Risk Treatment Decision (Mitigation/ Avoidance/ Transfer/ Acceptance)	Residual Risk	Contingency Plan	Due Date for Risk Treatment	Date Risk Treatment Implemented	Next Review Date	Closed Date	Comment
													Existing Control	Existing Control Effectiveness	Control Improvement Plan								

Risk Register Field Description

- **Risk**: Risk is the possibility or likelihood that a threat will exploit a vulnerability to cause harm to an asset and the severity of damage that could result.
- **Risk ID**: A sequential numeric identifier for referring to a risk in the risk register.
- **Risk Enlisting Date**: Date when the risk was first identified
- **Information Security Objective (s) Affected (confidentiality/ integrity /availability)**: The goals/objectives impacted by the risk to the organization in terms of confidentiality/ integrity /availability.
- **Linked/Consequence Risk**: Highlight whether the risk is linked to any other risk.
- **Risk description**: The title and description of the risk should be clearly recorded. Each risk description should outline the RISK EVENT, the CAUSE(S) and the IMPACT that could result from the reasonable worst-case scenario of the risk.
- **Vulnerability**: Vulnerability The weakness in an asset or the absence or the weakness of a safeguard or countermeasure is a vulnerability. In other words, a vulnerability is a flaw, loophole, oversight, error, limitation, frailty, or susceptibility that enables a threat to cause harm.
- **Threats**: Any potential occurrence that may cause an undesirable or unwanted outcome for an organization or for a specific asset is a threat.
- **Likelihood**: Estimate of how likely this is to occur.
- **Impact**: Estimate of how significant the impact of this risk will be if/when it becomes an issue.
- **Risk Rating**: Risk Rating is assessing the risks involved in the activities of an operation/ business and classifying them (VeryLow, Low, Medium, High, Very High) on the basis of the impact on the operation/business.
- **Priority**: A relative indicator of the criticality of this entry in the risk register, either expressed in ordinal value (e.g., 1, 2, 3) or in reference to a given scale (e.g. high, moderate, low)
- **Risk Owner**: Name of risk owner / senior accountable person Who would be responsible for managing the risk.
- **Risk Treatment**: This phase lays out risk treatment options to mitigate risk to an acceptable level. Mitigation, avoidance, transfer, and acceptance are some of the types of risk treatment options available to security teams. Cybersecurity controls are used to mitigate risks. New controls might be required or improved to properly mitigate future risk.
- **Residual risk**: After safeguards, security controls, and countermeasures are implemented, the risk that remains is known as residual risk.
- **Contingency plan**: A contingency plan is an alternative plan that will be used if a possible foreseen risk event becomes a reality. It is often used for risk management for an exceptional risk that, though unlikely, would have catastrophic consequences.
- **Due Date for Risk Treatment**: Timeline for Risk Treatment will be Implement.
- **Date of Risk Treatment Implemented**: Date of Risk Treatment Implemented.
- **Next review date**: Date when risk will next be reviewed / assessed / updated.
- **Closed date**: Date the risk was closed.

(মোঃ খায়রুল আমীন)
মহাপরিচালক
ডিজিটাল নিরাপত্তা এজেন্সি।