গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ
ডিজিটাল নিরাপত্তা এজেন্সি
আইসিটি টাওয়ার, আগারগাঁও, ঢাকা-১২০৭
www.dsa.gov.bd

তারিখ: ০২ মে, ২০২১

বিষয়: Critical Information Infrastrtucture (CII) গাইডলাইন এর খসড়া প্রেরণ সংক্রান্ত।

উপর্যুক্ত বিষয়ে ডিজিটাল নিরাপত্তা এজেন্সি হতে Critical Information Infrastrtucture (CII) গাইডলাইন এর খসড়া প্রস্তুত করা হয়েছে। প্রস্তুতকৃত খসড়া এর বিষয়ে পরবর্তী প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য খসড়াটি এতৎসঙ্গে প্রেরণ করা হলো।

০২-০৫-২০২১
(ছায়েদ আহম্মদ)
সিনিয়র পরামর্শক
ডিজিটাল নিরাপত্তা এজেন্সি

মহাপরিচালক
ডিজিটাল নিরাপত্তা এজেন্সি

তারিখ: ০২ মে, ২০২১

অনুলিপি সদয় জ্ঞাতার্থে ও কার্যার্থে প্রেরণ করা হলো:
১) পরিচালক (অপারেশন), অপারেশন অনুবিভাগ, ডিজিটাল নিরাপত্তা এজেন্সি।

[প্রাথমিক/পরীক্ষামূলক খসড়া। খসড়াটিতে পরিবর্তন/পরিমার্জন/পরিবর্ধন/সংশোধনের জন্য মতামত/মন্তব্য প্রয়োজন। এ সম্পর্কে প্রাপ্ত মতামত/মন্তব্যের ভিত্তিতে খসড়াটি চূড়ান্ত করা হবে।]

ডিজিটাল নিরাপত্তা এজেন্সি
তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ
ডাক, টেলিযোগাযোগ ও তথ্য প্রযুক্তি মন্ত্রণালয়
www.dsa.gov.bd

প্রজ্ঞাপন

তারিখ: ....., ১৪২৭ বঙ্গাব্দ/ ....., ২০২০ খ্রিস্টাব্দ

নং .....। 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 নিম্মরূপ গাইডলাইন প্রণয়ন করিল, যথা:-

অংশ-১

প্রারম্ভিক

১। শিরোনাম, প্রয়োগ ও প্রবর্তন।- (১) এই গাউলাইন গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা সুরক্ষার জন্য অনুশীলনীয়/অনুসরণীয় গাইডলাইন নামে অভিহিত হইবে।

(২) ভিন্নরূপ কোনো কিছু বলা না হইলে, এই গাউলাইনের 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 গাইড লাইন কার্যকর হইবে।

২। সংজ্ঞা।- বিষয় বা প্রসঙ্গের পরিপন্থি কোন কিছু না থাকিলে, এই গাইডলাইনে-

(১) “অপারেশনাল প্রযুক্তি” অর্থ পরস্পর সংযুক্ত কম্পিউটার ব্যবস্থা যাহার মাধ্যমে উহার ভৌত প্রক্রিয়া নিয়ন্ত্রণ ও পরিবীক্ষণ করা হয়;

(২) “আক্রম্যতা (vulnerability) নিরূপণ” অর্থ সিস্টেমের নিরাপত্তা আক্রম্যতা শনাক্ত ও নিরূপণ করা এবং যাহা হোস্ট নিরাপত্তা নিরূপণ, নেটওয়ার্ক নিরাপত্তা নিরূপণ ও নকশা পুন: নিরীক্ষণ (architecture review) সমন্বয়ে গঠিত;

(৩) “আইন” অর্থ ডিজিটাল নিরাপত্তা আইন, ২০১৮ (২০১৮ সনের ৪৬ নং আইন);

(৪) “এজেন্সি” অর্থ আইনের ধারা ৫ এর অধীন গঠিত ডিজিটাল নিরাপত্তা এজেন্সি;

(৫) “কম্পিউটার সিস্টেম” অর্থ আইনের ধারা ২(ঙ) তে সংজ্ঞায়িত কম্পিউটার সিস্টেম;

(৬) “গুরুত্বপূর্ণ তথ্য পরিকাঠামো” আইনের ধারা ২(ছ) তে সংজ্ঞায়িত গুরুত্বপূর্ণ তথ্য পরিকাঠামো;

(৭) “ডিজিটাল ডিভাইস” অর্থ আইনের ধারা ২(ঞ) তে সংজ্ঞায়িত ডিজিটাল ডিভাইস;

(৮) “ডিজিটাল নিরাপত্তা” আইনের ধারা ২(ট) তে সংজ্ঞায়িত ডিজিটাল নিরাপত্তা;

(৯) “ডিজিটাল নিরাপত্তার ঘটনা” অর্থ কম্পিউটার বা কম্পিউটার সিস্টেমের মাধ্যমে দৃষ্টিগ্রাহ্য কোনো কর্মকান্ড সংঘটন করা যাহা উক্ত কম্পিউটার বা কম্পিউটার সিস্টেম বা অন্য কোনো কম্পিউটার বা কম্পিউটার সিস্টেমের ডিজিটাল নিরাপত্তাকে ক্ষতিগ্রস্থ করিতে পারে, এবং ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনাও ইহার অন্তর্ভুক্ত হইবে;

(১০) “তথ্য প্রযুক্তি” অর্থ পরস্পর সংযুক্ত এমন একটি ব্যবস্থা যাহাতে তথ্য সংরক্ষণ, তথ্য নিবিষ্টকরণ (accessing), প্রক্রিয়াজাতকরণ; বিশ্লেষণ বা প্রেরণ করা হয়;

(১১) “দুর্ঘটনা পুনরুদ্ধার পরিকল্পনা: অর্থ তথ্য প্রযুক্তি বা অপারেশনাল প্রযুক্তি ব্যহত হইবার ক্ষেত্রে যে পদ্ধতিতে উহার সক্ষমতা পুনরুদ্ধার করা হয় সেই পদ্ধতি;

(১২) “দূর নিয়ন্ত্রণ প্রবেশ” অর্থ কোনো ব্যবহারকারী কর্তৃক বহিস্থ নেটওয়ার্ক যোগাযোগের মাধ্যমে গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রবেশ;

(১৩) “দূর নিয়ন্ত্রিত সুবিধাদি” অর্থ দূর নিয়ন্ত্রণের মাধ্যমে প্রবেশের সক্ষমতা রহিয়াছে এমন কম্পিউটার বা কম্পিউটার সিস্টেম;

(১৪) “নকশা পুন: নিরীক্ষণ (architecture review)” অর্থ সংকটাপূর্ণ সম্পদ, নেটওয়ার্ক ডিজাইনের দুর্বলতা, সংবেদশীল উপাত্ত সংরক্ষণ এবং সংকটাপূর্ণ আন্তসংযোগ ও এপ্লিকেশন নকশার ক্ষেত্রে নেটওয়ার্কে সম্ভাব্য হামলা ও আক্রম্যতা চিহ্নিত করিতে এপ্লিকেশনের ডিজাইন ও নেটওয়ার্ক নকশার পুন:নিরীক্ষণ ও বিশ্লেষণ;

(১৫) “নেটওয়ার্ক নিরাপত্তা নিরূপণ” অর্থ নেটওয়ার্কের নিরাপত্তার দুর্বলতা এবং কম্পিউটার বা কম্পিউটার সিস্টেমের নেটওয়ার্ক বহি:পরিসীমা (perimater) বা কম্পিউটার শনাক্ত ও মূল্যায়নের প্রক্রিয়া;

(১৬) “নেটওয়ার্ক জোন” অর্থ নিরাপত্তার শর্তাদি পূরণ করে এমন কম্পিউটার বা কম্পিউটার সিস্টেম সম্বলিত নেটওয়ার্কের যৌক্তিকভাবে বিভাজিত অংশ;

(১৭) “প্যাচ” অর্থ ডিজিটাল নিরাপত্তার আক্রম্যতা (vulnerability) অথবা উহার কার্যকরতা, ব্যবহারর্যতা বা কার্যক্ষমতার সহিত সংশ্লিষ্ট সফটওয়্যারের কোনরূপ পরিবর্তন করা;

(১৮) “পেনিট্রেশন টোস্টিং” অর্থ আক্রম্যতা অনুসন্ধানের মাধ্যমে প্রাপ্ত তথ্যের ভিত্তিতে কম্পিউটার সিস্টেম, নেটওয়ার্ক বা এপ্লিকেশনের নিরাপত্তা মূল্যায়নের জন্য অনুমোদিত প্রক্রিয়া;

(১৯) “বহিস্থ: কম্পিউটার বা কম্পিউটার সিস্টেম” অর্থ গুরুত্বর্পূণ তথ্য পরিকাঠামোর বহিস্থ: কোনো কম্পিউটার বা কম্পিউটার সিস্টেম, এবং উক্ত পরিকাঠামোর সহিত সংযোজিত দূরনিয়ন্ত্রিত সুবিধাদিও ইহার অন্তর্ভুক্ত হইবে;

(২০) “ব্যক্তি” অর্থে কোনো ব্যক্তি যিনি গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কোনো কার্য-সম্পাদন করেন, এবং উহার কর্মচারী, উহাতে সেবা প্রদানকরী বা অন্য কোনো তৃতীয় পক্ষও ইহার অন্তর্ভুক্ত হইবে;

(২১) “বিধিমালা” অর্থ আইনের অধীন প্রণীত ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০;

(২২) “ভেন্ডর” অর্থে প্রযুক্তি সরবরাহকারী ও সেবা প্রদানকারীও ইহার অন্তর্ভুক্ত হইবে;

(২৩) “মহাপরিচালক” ডিজিটাল নিরাপত্তা এজেন্সির মহাপরিচালক;

(২৪) “ম্যালওয়্যার” আইনের ধারা ২(ন) তে সংজ্ঞায়িত ম্যালওয়্যার;

(২৫) “সিকিউরিটি বেইজলাইন কনফিগারেশন স্টান্ডার্ড” অর্থ তথ্য প্রযুক্তি বা অপারেশন প্রযুক্তি জন্য লিখিত প্রক্ষেপনমালা যাহা কোনো এক সময় আনুষ্ঠানিকভাবে স্বীকৃত হইয়াছে;

(২৬) ”সেবা প্রদানকারী” আইনের ধারা ২(ফ) তে সংজ্ঞায়িত সেবা প্রদানকারী।

(২) এই আইনে ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞা এই গাইডলাইনে প্রদান কওরা 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

তথ্য প্রেরণ

৩। গুরুত্বপূর্ণ তথ্য পরিকাঠামো সংক্রান্ত তথ্য প্রদান।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো এই গাইডলাইন এ বর্ণিত নির্দেশাবলীর প্রতিপালন নিশ্চিত করিবে।

(২) আইন ও বিধিমালার উদ্দেশ্য পূরণকল্পে, মহাপরিচালক, নোটিশ দ্বারা, কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তাকে নিম্নবর্ণিত বিষয়ের যে কোনো তথ্যাদি প্রেরণের জন্য নির্দেশনা প্রদান করিতে পারিবে, এবং উক্তরূপে কোনো নির্দেশনা প্রদান করা হইলে সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহা প্রতিপালনে বাধ্য থাকিবে, যথা:-

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজাইন, বাহ্যিক আকার (configuration) ও নিরাপত্তা সম্পর্কিত-

(অ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে ব্যবহৃত প্রত্যেক প্রধান উপাদান (key component) ও আন্ত:সংযোগ নেটওয়ার্ক এর রেখাচিত্র (diagram) এবং উক্ত পরিকাঠামোর বহি:সংযোগের বিবরণ;

(আ) উক্ত পরিকাঠামোর প্রধান প্রধান উপাদানের নিম্নবর্ণিত বিষয়ের পূর্ণাঙ্গ বিবরণ-

(১) উহদের নাম ও বর্ণনা;

(২) উহাদের বাস্তব অবস্থান;

(৩) উহাতে ব্যবহৃত অপারোটিং সিষ্টেম ও উক্ত সিস্টেমের সংস্করণের (version) বিবরণ;

(৪) উহাতে ব্যবহৃত সফটওয়্যার ও উক্ত সফটওয়্যার এর সংস্করণের বিবরণ;

(৫) ইন্টারনেট প্রটোকলের ঠিকানা ও কোনো উপাদান যদি ইন্টারনেট ফেসিং হয়, তাহা হইলে উহার ওপেন পোর্ট এর বর্ণনা;

(৬) উক্ত পরিকাঠামো স্বয়ং অপারেটর না হইলে, সেইক্ষেত্রে অপারেটর এর নাম ও ঠিকানা;

(ই) উক্ত পরিকাঠামোতে প্রক্রিয়াজাতকৃত বা সংরক্ষিত উপাত্তের ধরন বা শ্রেণী;

(ঈ) উক্ত পরিকাঠামোর ডিজিটাল নিরাপত্তার দায়িত্বে নিয়োজিত সংশ্লিষ্ট সকল কর্মকর্তা/ব্যক্তির নাম ও যোগাযোগের ঠিকানা;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সহিত আন্ত:সংযোজিত কোনো কম্পিউটার বা কম্পিউটার সিস্টেমের ডিজাইন, বাহ্যিক আকার (configuration) ও নিরাপত্তা সম্পর্কিত নিম্নবর্ণিত তথ্য-

(অ) উক্ত কম্পিউটার বা কম্পিউটার সিস্টেমের নাম ও বিবরণ;

(আ) উহার বাস্তব অবস্থান;

(ই) অপারেটর এর নাম ও যোগাযোগের ঠিকানা;

(ঈ) কম্পিউটার বা কম্পিউটার সিস্টেম কর্তৃক প্রদত্ত কাজের বর্ণনা;

(উ) উক্ত পরিকাঠামোর সহিত বিনিময়কৃত উপাত্তের ধরন বা শ্রেণী;

(ঊ) উহাতে ব্যবহৃত অপারেটিং সিস্টেম ও সফটওয়্যার এর বর্ণনাসহ উহাদের সংস্করণের বিবরণ;

(ঋ) উহাতে ব্যবহৃত যোগাযোগ প্রটোকল এর বর্ণনাসহ কিভাবে উহা উক্ত পরিকাঠামোর সহিত সংযোজিত হইয়াছে উহার বিবরণ;

(গ) আউটসোর্সিং এর মাধ্যমে গৃহীত সেবার ধরন এবং সেবাদাতার নাম ও যোগাযোগের ঠিকানা;

(ঘ) মহাপরিচালক কর্তৃক, সময় সময়, নির্ধারিত অন্য কোন তথ্য।

অংশ-৩

ডিজিটাল নিরাপত্তা

৪। ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা অবহিতকরণ।- (১) যেক্ষেত্রে কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা সংঘটিত হয়, সেইক্ষেত্রে উক্ত পরিকাঠামোর দায়িত্ব প্রাপ্ত ব্যক্তি/কর্মকর্তা সংঘটিত ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা সম্পর্কে উপ-অনুচ্ছেদ (২) এ বর্ণিত পদ্ধতিতে, লিখিতভাবে, মহাপরিচালকে অবহিত করিবে, যথা:-

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামো ক্ষতিগ্রস্থ হইবার বিস্তারিত বিবরণ;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নাম এবং ক্ষতিগ্রস্ত ব্যক্তির নাম ও যোগাযোগের ফোন নম্বর;

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

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

(ঙ) উক্ত ঘটনা অবহিতকারীর নাম ও ফোন নম্বর ও পদবী।

(২) উপ-অনুচ্ছেদে (১) এ উল্লিখিত তথ্য ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা সংঘটিত হইবার ৭ (সাত) দিন এর মধ্যে বা মহাপরিচালক কর্তৃক নির্ধারিত সময়ের মধ্যে উক্ত ঘটনা সংঘটিত হইবার কারণ, উক্ত কারণে উক্ত পরিকাঠামো বা উহার কম্পিউটার বা কম্পিউটার সিস্টেম উপর সৃষ্ট প্রভাব এবং এতদসম্পর্কিত অন্যান্য সম্পুরক তথ্য, লিখিতভাবে, সরাসরি মহাপরিচালক কর্তৃক নির্দিষ্টকৃত নম্বরে ফোন করিয়া বা টেক্সট মেসেজ প্রদান করিয়া বা এজেন্সির ওয়ের সাইটে বিধৃত ফরম পূরণ করিয়া প্রেরণ করিতে হইবে।

৫। ডিজিটাল নিরাপত্তা ঝুঁকি নিরূপণ।- (১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরাপত্তা ঝুঁকি নিরূপণের ক্ষেত্রে, বাস্তবতার নিরীখে, যতদূর সম্ভব, উক্ত পরিকাঠামোর নিরাপত্তার ঝুঁকিসহ উহা নিরসনে উক্ত পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা কর্তৃক কি কি ব্যবস্থা গ্রহণ করা হইবে উহা চিহ্নিতপূর্বক সম্ভাব্য ঘটনার ফলাফল বা প্রভাব মূল্যায়ন করিতে হইবে।

(২) উপ-অনুচ্ছেদ (১) অধীন নিরাপত্তা ঝুঁকি চিহ্নিতকরণ ও মূল্যায়নের পর উক্ত পরিকাঠামো উক্ত বিষয়ে মহাপরিচালকের নিকট প্রেরণ করিবে, এবং উক্ত প্রতিবেদনে, অন্যান্য বিষয়ের মধ্যে, নিরাপত্তা ঝুঁকি নিরূপণে ব্যবহৃত পদ্ধতি (methodology), নিরাপত্তা ঝুঁকি নিরূপণ চিহ্নিতকরণের বিস্তারিত বিবরণ এবং উক্ত বিষয়ে উক্ত পরিকাঠামো কর্তৃক গৃহীত ব্যবস্থাদি অন্তর্ভুক্ত থাকিবে।

(৩) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো মহাপরিচালক কর্তৃক নির্ধারিত সময়ের মধ্যে উহার ডিজিটাল নিরাপত্তা ঝুঁকি নিরূপণ করিয়া তৎসম্পর্কে উপ-অনুচ্ছেদ (২) এ বর্ণিত প্রতিবেদন মহাপরিচালকের নিকট প্রেরণ করিবে।

৬। নিরাপত্তা ঝুঁকি নিরসনে গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কর্মরত ব্যক্তি/কর্মকর্তার দায়িত্ব নির্ধারণ।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর প্রয়োজনীয় ডিজিটাল নিরাপত্তা 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) উক্ত পরিকাঠামোর ডিজিটাল নিরাপত্তা ব্যবস্থার সাংঘটনিক কাঠামো;

(খ) উক্ত পরিকাঠামোতে কর্মরত প্রত্যেক ব্যক্তির/কর্মকর্তার কার্যাবলী সুনির্দ্দিষ্টকরণ সংক্রান্ত তথ্য;

(গ) আইন, বিধিমালা ও এই গাইডলাইনে বিধৃত নির্দেশনা প্রতিপালনের জন্য দায়ী ব্যক্তি/কর্মকর্তা নির্দ্দিষ্টকরণ।

৭। ঝুঁকি ব্যবস্থাপনা।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো, লিখিতভাবে, ডিজিটাল নিরাপত্তা ঝুঁকি ব্যবস্থাপনার জন্য একটি কাঠামো (famework) প্রস্তুত করিবে, এবং উক্ত কাঠামোতে, অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত বিষয়াদি অন্তর্ভুক্ত থাকিবে, যথা:-

(ক) ডিজিটাল নিরাপত্তা ঝুঁকি ব্যবস্থাপনার দায়িত্বে নিয়োজিত ব্যক্তি/কর্মকর্তাগণের 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 নিরূপণের পরিবীক্ষণ ব্যবস্থা।

(২) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো শনাক্তকৃত (identified) ডিজিটাল নিরাপত্তা ঝুঁকির একটি তালিকা সংরক্ষেণের উদ্দেশ্যে একটি ঝুঁকি রেজিস্টার সংরক্ষণ করিবে, এবং উক্ত রেজিস্টারে নিম্নবর্ণিত তথ্যাদি নিয়মিতভাবে লিপিবদ্ধ ও হালনাগাদ রাখিতে হইবে, যথা:-

(ক) ঝুঁকি শনাক্তকরণের তারিখ;

(খ) ঝুঁকির বিবরণ;

(গ) ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনার অনুরূপ কোনো ঘটনা সংঘটনের বিবরণ;

(ঘ) ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনার তীব্রতা;

(ঙ) ঝুঁকি নিরসনের বিবরণসহ উহার সর্বশেষ অবস্থান;

(চ) সর্বশেষ (residual) ঝুঁকির বিবরণ।

(৩) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) নিয়মিতভাবে শনাক্তকৃত সকল নিরাপত্তা ঝুঁকির বিবরণ লিপিবদ্ধক্রমে উহার পরিবীক্ষণ নিশ্চিত করিবে;

(খ) এই গাইডলাইন, আইনগতভাবে প্রতিপালনীয় ডিজিটাল নিরাপত্তার শর্তাদি (requirement) ও ডিজিটাল নিরাপত্তা সাংক্রান্ত জাতীয় নীতির সহিত সামজস্যপূর্ণভাবে উক্ত পরিকাঠামোর নিরাপত্তা ঝুঁকি ও সুরক্ষার বিষয়াদি ব্যবস্থাপনার জন্য তৎকর্তক পালনীয় নীতি নির্দেশনা ও মানদন্ড নির্ধারণ করিবে; এবং

(গ) উহার সিস্টেমের জীবনচক্রের উন্নয়নের নিমিত্ত ডিজিটাল নিরাপত্তা ডিজাইন কাঠামো (Security By Design Framework) গ্রহণ/অনুসরণ করিবে।

অংশ-৪

ডিজিটাল নিরাপত্তা ব্যবস্থার নিরীক্ষা/অডিট

৮। ডিজিটাল নিরাপত্তা ব্যবস্থা নিরীক্ষার বাধ্যবাধকতা।- (১) আইন ও বিধিমালাতে এতদসংক্রান্ত বিধৃত বিধি-বিধানের আলোকে, প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা, মহাপরিচালক কর্তৃক নির্দ্দিষ্টকৃত সময়ের মধ্যে, স্বাধীনভাবে, তাহার নিয়ন্ত্রণাধীন পরিকাঠামোর ডিজিটাল নিরাপত্তার নিরীক্ষার ব্যবস্থা করিবে, এবং উক্ত নিরীক্ষার মুখ্য উদ্দেশ্য হইবে আইন, বিধিমালা, এই গাইডলাইনের বিধান এবং মহাপরিচালক কর্তৃক, সময় সময়, জারীকৃত আদর্শ পরিচালনা পদ্ধতি (SOP), কর্ম-সম্পাদনের মানদন্ড ও নির্দেশনা প্রতিপালিত হইতেছে কিনা উহা নিরূপণ করা।

(২) উপ-অনুচ্ছেদে (১) এর অধীন নিরীক্ষা কার্য সম্পন্নের ১৫ (পনের) দিনের মধ্যে প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা নিরীক্ষা প্রতিবেদনের অনুলিপি মহাপরিচালকের নিকট প্রেরণ করিবে।

(৩) উপ-অনুচ্ছেদ (১) এ যাহা কিছুই থাকুক না কেন, মহাপরিচালক, উক্ত উপ-অনুচ্ছেদের উদ্দেশ্যে পূরণকল্পে, আদেশ দ্বারা, তৎকর্তৃক নিযুক্ত নিরীক্ষক দ্বারা কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে আইন, বিধিমালা, এই গাইডলাইনের বিধান অনুসরণক্রমে নিরীক্ষা কার্য সম্পন্ন করিবার জন্য নির্দেশ দিতে পারিবে, এবং উত্তরূপে কোন নির্দেশ প্রদান করা হইলে, সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা নিরীক্ষা কার্য সম্পন্ন করিবার ব্যাপারে নিরীক্ষককে পূর্ণ সহযোগীতা করিতে বাধ্য থাকিবে।

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

৯। সংশোধনী পরিকল্পনা।- (১) অনুচ্ছেদে ৮ এর অধীন পরিচালিত নিরীক্ষায় যদি চিহ্নিত হয় যে, গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনায় আইন, বিধি ও এই গাইডলাইনের বিধান এবং মহাপরিচালক কর্তৃক জারিকৃত আদর্শ পরিচালন পদ্ধতি, কার্য-সম্পাদনের মানদন্ড বা নির্দেশনা যথাযথভাবে প্রতিপালিত হইতেছে না, তাহা হইলে মহাপরিচালক এতদদ্দেশ্যে ভিন্নরূপ কোনো নির্দেশনা প্রদান না করিলে, গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা নিরীক্ষা প্রতিবেদন প্রাপ্তির ১৫ (পনের) দিনের মধ্যে মহাপরিচালকের নিকট উক্ত পরিকাঠামো পরিচালনা সংক্রান্ত একটি সংশোধনী পরিকল্পনা উপস্থাপন করিবে, এবং উক্ত পরিকল্পনায় কিভাবে নিরীক্ষায় চিহ্নিতকৃত বিষয়সমূহের প্রতিপালন যথাযথভাবে অনুসৃত হইবে উহার কর্ম-পরিকল্পনার বিবরণসহ উহা উত্তরণের সময়সীমার উল্লেখ থাকিবে।

(২) মহাপরিচালক, উক্ত পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তার সহিত আলোচনাক্রমে, প্রয়োজনে, তৎপ্রেক্ষিতে দাখিলকৃত সংশোধনী পরিকল্পনা পরিমার্জনক্রমে নূতন পরিকল্পনা দাখিলের জন্য নির্দেশ প্রদান করিতে পারিবে, এবং এইরূপে দাখিলকৃত পরিমার্জিত সংশোধনী পরিকল্পনা মহাপরিচালক কর্তৃক অনুমোদিত হইলে উক্ত পরিকাঠামোর দায়িত্বেপ্রাপ্ত ব্যক্তি/কর্মকর্তা উহার ভিত্তিতে নিজ খরচে উক্ত পরিকাল্পনা বাস্তবায়ন করিবে।

অংশ-৫

পরিসম্পদ ব্যবস্থাপনা

১০। পরিসম্পদ ব্যবস্থাপনা।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা তাহার তত্তাবধানাধীন পরিকাঠামোর পরিসম্পদ চিহ্নিতপূর্বক উক্ত পরিসম্পদের একটি তালিকা সমন্বয়ে একটি রেজিস্টার সংরক্ষণ করিবেন, এবং উক্ত তালিকায়, অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত বিষয়াদি অন্তর্ভুক্ত থাকিবে।

(ক) পরিসম্পদের নামসহ উহার বিস্তারিত বিবরণ;

(খ) পরিসম্পদের গুরুত্বপূর্ণ কার্যাবলি;

(গ) উক্ত পরিসম্পদ ব্যবহারকারী অপারেটরের নাম;

(ঘ) পরিসম্পদের ভৌত বা ব্যবহারিক অবস্থান;

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

(২) প্রত্যেক গুরুত্বপূণ্য 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।

(৩) এই অনুচ্ছেদে বর্ণিত রেজিষ্টারে অন্তর্ভুক্ত তালিকাভুক্ত পরিসম্পদ অনুচ্ছেদ ৫ এর অধীন ডিজিটাল নিরাপত্তা ঝুঁকি নিরূপণের আওতাভুক্ত হইবে।

অংশ-৬

সুরক্ষা সংক্রান্ত বিষয়াদি

১১। প্রবেশাধিকার নিয়ন্ত্রণ।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কেবল উক্ত পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা কর্তৃক অনুমোদিত ব্যক্তির প্রবেশাধিকার সীমিত থাকিবে এবং কোনো ব্যক্তি উক্ত দায়িত্বপ্রাপ্ত ব্যক্তি/কার্মকর্তা কর্তৃক অনুমোদিত নয় এমন কোনো কর্মকান্ড পরিচালনা করা যাইবে না, এবং উক্ত পরিকাঠামোতে প্রবেশের ক্ষেত্রে ডিজিটাল নিরাপত্তা ঝুঁকির সহিত সামঞ্জস্যপূর্ন প্রমাণীকরণ কৌশল (authentication technique) প্রয়োগ করিতে হইবে।

(২) প্রবেশাধিকার নিয়ন্ত্রণের উদ্দেশ্যে, গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা তাহার নিয়ন্ত্রণাধীন পরিকাঠামোতে সকল প্রবেশ সংক্রান্ত তথ্যের তালিকা (log) সংরক্ষণ করিবে, এবং ডিজিটাল নিরাপত্তা ঝুঁকির সহিত সামঞ্জস্যপূর্ণভাবে উক্ত পরিকাঠামোতে প্রবেশের ক্ষেত্রে ইলেকট্রনিক প্রমানীকরণ কৌশল স্থাপন করিবে।

(৩) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তার প্রত্যক্ষ তত্ত্বাবধানে কেবল উক্ত পরিকাঠামোর ইন্টারফেস (যেমন: ইউএসবি পোর্ট, সিরিয়াল পোর্ট, ইত্যাদি) ও ভেন্ডর সার্ভিস এপ্লিকেশন এ প্রবেশ করা যাইবে, এবং সম্ভাব্য ক্ষেত্রে উক্ত ব্যক্তি/কর্মকর্তার সরাসরি নজরদারীর ভিত্তিতে কার্য-সম্পাদন করিতে হইবে।

১২। সিস্টেম দৃঢ়করণ (hardening)।- (১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা ব্যবস্থার সহিত সংগতিপূর্ণভাবে উক্ত পরিকাঠামোর অপারেটিং সিস্টেম, এপ্লিকেশন ও নেটওয়ার্ক যন্ত্রপাতির জন্য সিকিউরিটি বেইজলাইন কনফিগারেশন স্টান্ডার্ড প্রতিষ্ঠা করিতে হইবে, এবং উহাতে, অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত নিরাপত্তার নীতির প্রতিফলন থাকিতে হইবে, যথা:-

(ক) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রবেশের সুযোগ সীমিত কওরা এবং উক্ত বিষয়ে দায়িত্ব পালনরত ব্যক্তিগণের দায়িত্ব সুনির্দিস্টকরণ;

(খ) পাসওয়ার্ড এর ব্যবহার নীতি কার্যকরকরণ;

(গ) অব্যবহৃত একাউন্টস অপসারণ;

(ঘ) অপ্রয়োজনীয় সেবা ও ভেন্ডর সাপোর্ট এপ্লিকেশনসহ অন্যান্য এপ্লিকেশন অপসারণ;

(ঙ) অব্যবহৃত নেটওয়ার্ক পোর্ট বন্ধকরণ;

(চ) ম্যালওয়ার এর বিরুদ্ধে সুরক্ষা;

(ছ) সিস্টেম ভেন্ডর কর্তৃক অনুমোদিত সফটওয়্যার ও নিরাপত্তা প্যাচ হালনাগাদকরণ।

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা তাহার নিয়ন্ত্রণাধীন পরিকাঠামোতে ব্যবহৃত বিদ্যমান যন্ত্রপাতির সহিত নূতন কোনো যন্ত্রপাতি সংযোজন বা পরিবর্তনের ক্ষেত্রে আবশ্যিকভাবে উপ-অনুচ্ছেদ (১) এ উল্লিখিত স্টান্ডার্ড এর প্রয়োগ নিশ্চিত করিবে।

(৩) প্রতিবৎসর অন্তত একবার প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার সিকিউরিটি বেইজলাইন কনিফগারেশন স্টান্ডার্ড মূল্যায়ন করিবে।

(৪) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে আনীত সকল ধরনের সিস্টেমের পরিবর্তনকে প্রাধিকার ও বৈধতা দানের ক্ষেত্রে উহা পরিবর্তিত ব্যবস্থাপনা প্রক্রিয়া (change management process) অনুসরণ করিবে।

১৩। দূর নিয়ন্ত্রণ সংযোগ ব্যবস্থা।- (১) অবৈধ অনুপ্রবেশ প্রতিরোধ ও উহা শনাক্তের জন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সকল দূর নিয়ন্ত্রিত সংযোগ ব্যবস্থার কার্যকর ডিজিটাল নিরাপত্তা ব্যবস্থা থাকিতে হইবে-

(২) দূর নিয়ন্ত্রণ সংযোগের ক্ষেত্রে নিম্নবর্ণিত ব্যবস্থাদির অনুশীলন নিশ্চিত করিতে হইবে-

(ক) প্রয়োজনীয়তার নিরীখে, সম্ভাব্য ক্ষেত্রে, দূরবতী স্থান হইতে সংযোগ স্থাপন;

(খ) লভ্যতার (avilable) ক্ষেত্রে, দৃঢ় প্রমাণীকরণ কৌশল (authentication technique), নিরাপত্তা সঞ্চালন (transmission) ও মেসেজের শুদ্ধতা (integrity) বাস্তবায়ন;

(গ) সকল নেটওয়ার্ক সংযোগের জন্য এনক্রিপশন বন্তবায়ন;

(ঘ) ব্যবহারিক প্রয়োজনীয়তা না হইলে, গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে প্রভাবিত করিতে পারে এমন সিস্টেম কমান্ড হইতে দূর-নিয়ন্ত্রণ সংযোগ প্রদানে অসন্মতি জ্ঞাপন;

(ঙ) সংযোগের জন্য প্রয়োজনের অতিরিক্ত উপাত্তের প্রবাহ সীমাবদ্ধকরণ।

১৪। অপসারণযোগ্য স্টোরেজ মিডিয়া।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো ব্যবস্থাদি গ্রহণক্রমে অপসারণযোগ্য স্টোরেজ মিডিয়া ও বহনযোগ্য কম্পিউটার ডিভাইস এর উপর সুস্পষ্ট নিয়ন্ত্রণ ব্যবস্থা গ্রহণ করিতে হইবে।

(২) অপসারণযোগ্য স্টোরেজ মিডিয়ার সংরক্ষিত সকল সংবেদনশীল তথ্য এনক্রিপটেড হইতে হইবে।

১৫। আক্রম্যতা (vulnerabililty) নিরূপণ, ইত্যাদি।- (১) নিরাপত্তা ও নিয়ন্ত্রণ ব্যবস্থার দুর্বলতা চিহ্নিতকরণের উদ্দেশ্যে, প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো, মহাপরিচালক কর্তৃক নির্দিষ্টকৃত সময়ের মধ্যে, উহার আইটি বা ওটি সিস্টেমের আক্রম্যতা নিরুপণের ব্যবস্থা করিবে, এবং উক্ত ক্ষেত্রে হোস্ট ও নেটওয়ার্ক নিরাপত্তা ব্যবস্থা নিরূপণ এবং নিরাপত্তার নকশা পুনরীক্ষণসহ উহার আইটি সিস্টেমের পেনিট্রেশন টেস্ট করিবে।

(২) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে অধিকতর গুরুত্বপূর্ণ নূতন আইটি সিস্টেম সংযোজন বা এপ্লিকেশন মডিউল, সিস্টেম আপগ্রেড বা প্রযুক্তিগত রিফ্রেশ পরিবর্তন বা সংযোজনের ক্ষেত্রে এবং চিহ্নিত আক্রম্যতা নিরূপণের জন্য গতিবিধি অনুসরণের জন্য উপ-অনুচ্ছেদ (১) উল্লিখিত ব্যবস্থাদি প্রহণ করিতে হইবে।

(৩) উপ-অনুচ্ছেদ (১) ও (২) এ উল্লিখিত পেনিট্রেশন টেস্ট উহার প্রযুক্তিগত লভ্যতার ভিত্তিতে সম্পন্ন করা যাইবে এবং কোনো তৃতীয় পক্ষের মাধ্যমে উক্ত টেস্ট করার ক্ষেত্রে উহা উক্ত পরিকাঠামোর সরাসরি তত্ত্বাবধানে সম্পন্ন করিতে হইবে।

(৪) মহাপরিচালক কর্তৃক নির্দেশিত হইলে প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো আক্রম্যতা নিরূপণ ও পেরিট্রেশন টেস্ট এর ফলাফল অনতিবিলম্বে তাহার নিকট প্রেরণ করিবে।

অংশ-৭

ডিজিটাল নিরাপত্তা বিঘ্নিত হহইবার ঘটনা শনাক্তকরণ ও প্রতিরোধকরণ

১৬। শনাক্তকরণ।- (১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সহিত সম্পর্কযুক্ত ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা চিহ্নিতকরণ, শনাক্তকৃত ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা বিশ্লেষণ ও তুলনাকরণ, এবং ইতিমধ্যে 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) উপ-অনুচ্ছেদ (১) এর উদ্দেশ্য পূরণকল্পে, প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর উক্ত উপ-অনুচ্ছেদের অধীন প্রণীত কার্য-সম্পাদন ও তথ্য আহরণ প্রক্রিয়ার কার্যকরতা নিরূপনার্থ মহাপরিচালক কর্তক নির্ধারিত সময়ের মধ্যে অন্তত একবার উহা মূল্যায়ন ও পর্যালোচনা করিবে।৮

১৭। ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনার প্রতিরোধ পরিকল্পনা।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা প্রতিরোধের জন্য একটি সমান্বিত প্রতিরোধ পরিকল্পনা (respouce plan) প্রস্তুত করিবে, এবং উহাতে, অন্যন্য বিষয়ের মধ্যে, নিম্নবর্ণিত বিষয়াদি অন্তর্ভুক্ত থাকিবে, যথা:-

(ক) "সাইবার ইন্সিডিন্ট রেসপন্স টীম" এর গঠন কাঠামো এবং উক্ত টীমের সমস্যগণের দায়িত্ব, কার্যবলী ও তাহাদের সহিত যোগাযোগের বিবরণ এবং উক্ত ঘটনার প্রতিরোধ সীমা ও পদ্ধতি নির্ধারণ;

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

(গ) নিরাপত্তা বিঘ্নিত হইবার ঘটনার প্রভাব নিয়ন্ত্রন এবং উহার পুনরুদ্ধার প্রক্রিয়া কার্মকরকরণ;

(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 যন্তপাতি 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 অধীন প্রণীত পরিকাল্পনা সম্পর্কে উক্ত পরিকাঠামোর সহিত সংশ্লিষ্ট সকল ব্যক্তিকে উহার কার্যকরতা সম্পর্কে অবহিতক্রমে প্রয়োজনীয়তার নিরীখে উহা পর্য্যালোচনা ও মূল্যায়ন করিবে।

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

(ক) কোনো সংকটের সময় সহজে কার্যকর যোগাযোগ ব্যবস্থা গড়িয়া তুলবার জন্য ‘ক্রইমাস কমিউনিকেশন টীম’ নামে একটি টীম গঠন করিবে;

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

(গ) প্রতিনিধিত্বকারী ফোকাল পয়েন্ট হিসাবে একজন কারিগরি বিশেষজ্ঞ 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) উক্তরূপ পরিকল্পনা যথাযথভাবে কার্যকর করিবার উদ্দেশ্যে নিয়মিত অনুশীলনের ব্যবস্থা গ্রহণ করিবে।

অংশ-৮

ডিজিটাল নিরাপত্তা সংক্রান্ত তথ্য বিনিময়, সচেতনতা সৃষ্টি, ইত্যাদি

১৯। ডিজিটাল নিরাপত্তা ব্যবস্থা সম্পর্কে সচেতনতা সৃষ্টি।- প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার সকল কর্মচারী, ভেন্ডর ও উক্ত পরিকাঠামোতে প্রবেশাধিকার রহিয়াছে এমন সকল ব্যক্তির ডিজিটাল নিরাপত্তা ব্যবস্থা সম্পর্কে সচেতনতা সৃষ্টির জন্য একটি কর্মসূচী গ্রহণ করিবে, এবং উক্ত কর্মসূচী উক্ত পরিকাঠামোর সহিত সংশ্লিষ্ট সকল শ্রেণীর কর্মচারি, 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 ব্যবস্থা গ্রহণ করিবে।

২০। তথ্য বিনিময়।- প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামোর দায়িত্বপ্রাপ্ত ব্যক্তি/কর্মকর্তা তাহাদের আওতাধীন পরিকাঠামো সম্পর্কিত নিরাপত্তা বিঘ্নিত হইবার ঘটনা, নিরাপত্তার হুমকি এবং তৎসংক্রান্ত বিষয়ে গৃহীত ব্যবস্থা সম্পর্কিত তথ্য উক্ত পরিকাঠামোর সহিত সংশ্লিষ্ট সকল ব্যক্তি, ভেন্ডর, সেবা প্রদানকারীর সহিত বিনিময় করিবে এবং তদুদ্দেশ্যে যথাযথ ব্যবস্থা গ্রহণ করিবে।

২১। ডিজিটাল নিরাপত্তা ব্যবস্থার অনুশীলন।- (১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো মহাপরিচালক কর্তৃক নির্দেশিত পদ্ধতিতে নিয়মিত ডিজিটাল নিরাপত্তা ব্যবস্থার অনুশীলন করিবে।

(২) উক্ত অনুশীলনে ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা প্রতিরোধ সংক্রান্ত টীমের সকল সদস্যকে অংশ গ্রহণ করিবে।

(৩) উক্তরূপ অনুশীলন সংক্রান্ত কোনো তথ্য প্রদানের ব্যাপারে মহাপরিচালক কর্তৃক অনুরূদ্ধ হইলে প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহার ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা প্রতিরোধ, সংকটকালীন যোগাযোগ ব্যবস্থার পরিকল্পনা এবং পরিচালন পদ্ধতি সংক্রান্ত সকল তথ্য মহাপরিচালকের নিকট প্রেরণ করিতে হইবে।

অংশ-৯

ভেন্ডর ব্যবস্থাপনা, ইত্যাদি

২২। ভেন্ডর ব্যবস্থাপনা।- (১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রবেশ ওতথ্য 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 অন্তর্ভুক্ত করিতে হইবে, এবং উহাতে, অন্যান্য বিষয়ের মধ্যে, নিরাপত্তা হুমকি প্রতিরোধের ক্ষেত্রে করণীয় সংক্রান্ত বিষয়ের অন্তর্ভুক্ত থাকিবে।

(২) গুরুত্বপূর্ণ তথ্য পরিকামো ভেন্ডর বা সেবা প্রদানকারীর ডিজিটাল নিরাপত্তা ব্যবস্থার সহিত সংশ্লিষ্ট সকল পণ্যের বৈধতা প্রদানের পদ্ধতি নির্ধারণ করিবে।

(৩) প্রত্যেক গুরুত্বপূণ তথ্য পরিকাঠামো আউট সোসিং এর মাধ্যমে উহার নিরাপত্তা ব্যবস্থা রক্ষণাবেক্ষণ করিতে পারিবে।

অংশ ১০

পরিচালনাগত প্রযুক্তি ব্যবস্থা

(এই অংশ কেবল অপারেশনাল প্রযুক্তি ব্যবস্থার ক্ষেত্রে প্রযোজ্য)

(ক) নেটওয়ার্ক বিভাজন:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামো 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 ক্ষেত্রে উক্ত পরিকাঠামো ও যে নেটওয়ার্ক জোনে কোনো তথ্য বা উপাত্ত প্রেরণ করা হইবে সেই নেটওয়ার্ক জোনের মধ্যে যোগাযোগ সীমাবদ্ধ রাখিতে হইবে।

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

(খ) প্রবেশাধিকার নিয়ন্ত্রণ:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে দায়িত্ব ভিত্তিক প্রবশাধিকার নিয়ন্ত্রণের ব্যবস্থাসহ উক্ত ব্যবস্থার সঠিক প্রয়োগ নিশ্চিত করিবার জন্য নিয়মিতভাবে উক্ত ব্যবস্থা পর্য্যালোচনা ও পরিবীক্ষণ করিতে হইবে।

(২) যেক্ষেত্রে গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনার জন্য যৌথ ইউজার একাউন্ট এর প্রয়োজন হয়, সেইক্ষেত্রে উক্ত একাউন্টে অবৈধ অনুপ্রবেশ রোধ করিবার জন্য নিয়মিতভাবে উক্ত একাউন্টসমূহের ব্যবহারিক প্রয়োগ পর্য্যালোচনা ও পরিবীক্ষণের জন্য যথাযথ পদ্ধতি অনুসরণ করিবে।

(৩) গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) উহার ব্যবহারিক কর্মকান্ড পর্য্যবেক্ষণের জন্য ইউজার এ্যকটিভিটি লগ রক্ষণাবেক্ষণ করাসহ অস্বাভাবিক কর্মকান্ড পর্যবেক্ষণের জন্য উক্ত লগ ব্যবস্থা নিয়মিতভাবে পুনরীক্ষণ করিবে; এবং

(খ) উহার পরিসম্পদ ব্যবস্থাপনা সংক্রান্ত প্রিভিলেজ একাউন্টসমূহের জন্য বহুমুখী প্রমাণীকরণ ব্যবস্থা গ্রহণ করিবে।

(গ) নেটওয়ার্ক এর নিরাপত্তা ব্যবস্থা:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

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

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

(ঘ) এপ্লিকেশন এর নিরাপত্তা ব্যবস্থা:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) উহাতে ব্যবহারের জন্য অনুমোদিত এপ্লিকেশন এর তালিকা প্রস্তুত করিতে হইবে, এবং উক্ত তালিকায় কেবল উক্ত পরিকাঠামোর পরিচালনাগত ও ডিজিটাল নিরাপত্তা ব্যবস্থার প্রয়োজনীয় এপ্লিকেশন এর সংস্থান থাকিতে হইবে;

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

(গ) যথাযথভাবে যাচাই প্রক্রিয়ার মাধ্যমে বৈধ উৎস হইতে এপ্লিকেশন ও প্যাটসমূহ সংগ্রহ ও ব্যবহারের উপযোগি করিবে।

(ঙ)প্যাচ ব্যবস্থাপনা:

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

(ক) পরিচালনা, আক্রম্যতা, পরিবর্তন ও ব্যহ্যিক আকার (configaration) ব্যবস্থাপনা, ব্যাক আপ, পরীক্ষণ, নিরাপত্তা বিঘ্নিত হইবার ঘটনার রেসপন্স, বিপর্যয় পুনরুদ্ধার, ইত্যাদি প্রক্রিয়ার সহিত প্যাচ ব্যবস্থাপনার সমন্বয়ের কৌশল;

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

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

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

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

(চ) অপসারণযোগ্য স্টোরেজ মিডিয়া:

গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সহিত সম্পর্কিত সকল কর্মক্ষেত্রে উপাত্ত স্থানান্তর করার ক্ষেত্রে কেবল অনুমোদিত অপসারণযোগ্য স্টোরেজ মিডিয়ার ব্যবহার করিতে হইবে।

(ছ) পরিবীক্ষণ ও শনাক্তকরণ:

প্রতেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো-

(ক) উহার লগ সংক্রান্ত সকল ঘটনার জন্য উক্ত পরিকাঠামো একটি কনসিসটেন্ট টাইম সোর্স ব্যবহার,

(খ) উহার স্বভাবিক পরিচালানার জন্য উক্ত পরিকাঠামোর প্রত্যাসিত নেটওয়ার্ক প্রবাহ ও কার্য-সম্পাদন প্রক্রিয়ার ভিত্তিরেখা প্রস্তুত,

(গ) ডিজিটাল নিরাপত্তা ব্যবস্থার হুমকি নিয়ন্ত্রণে দৃষ্টিগ্রাহ্য নিয়ন্ত্রণ এবং উক্তরূপ নিরাপত্তা ব্যবস্থার ধারাবাহিক পরিবীক্ষণের ব্যবস্থা গ্রহণ,

করিতে হইবে।

অংশ-১১

অনুশীলনীয়/অনুসরণীয় উত্তম চর্চা

২৩। অনুশীলনীয়/অনুসরণীয় উত্তম চর্চা।- প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো কর্তৃক উহার নিরাপত্তা ব্যবস্থার সুরক্ষার ক্ষেত্রে নিম্নবর্ণিত উত্তম চর্চা অনুসরণ করিবে, যথা:-

(ক) পরিকল্পনার মাধ্যমে নিয়ন্ত্রণ:

(i) পরিকল্পনা বিষয়ক:

(১) 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;

(২) আইনগত ও নিয়ন্ত্রণমূলক ব্যবস্থাদি অনুধাবন করা;

(৩) তথ্য নিরাপত্তার কর্ম পরিকল্পনার ব্যবস্থাপনা, রক্ষণাবেক্ষণ, ইত্যাদির জন্য প্রয়োজনীয় আর্থের সংস্থান করা;

(৪) ISO/IEC 27001 স্ট্যান্ডার্ড অনুসরণে তথ্য নিরাপত্তা ব্যবস্থাপনার সিস্টেমের নিরাপত্তা ঝুঁকি ব্যবস্থাপনার কাঠামো নির্ধারণ।

(ii) উন্নয়ন বিষয়ক:

(১) তথ্য নিরাপত্তার ব্যবস্থার উন্নয়নে যথাযথ নীতি, মানদন্ড, গাইড লাইন ও পদ্ধতি নির্ধারণ করা;

(২) তথ্য নিরাপত্তা ব্যবস্থার দলিলাদি প্রণয়ন করা এবং উহা পর্য্যালোচনা, হালনাগাদ ও আনুষ্ঠানিকভাবে বাস্তবায়ন করা;

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

(৪) উপরি-উক্ত কার্যাদি সম্পাদনে সংশ্লিষ্ট অংশীজনের পরামর্শ গ্রহণ।

(iii) ব্যবস্থাপনা বিষয়ক:

(১) তথ্য নিরাপত্তার নীতি, পদ্ধতি ও গাইড লাইন প্রচারের ব্যবস্থা করা;

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

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

(৪) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কর্ম-সম্পাদন (business) প্রক্রিয়ার সহিত তথ্য নিরাপত্তা ব্যবস্থার অঙ্গীভূত (integration) করা;

(৫) তথ্য নিরাপত্তা ব্যবস্থার নীতি, মানদন্ড, পদ্ধতি, ইত্যদির কার্যকরতার মূল্যায়ন ও পর্য্যালোচনা করা;

(৬) তথ্য নিরাপত্তা বিঘ্নিত হইবার ঘটনাসমূহের বিবরণের রেকর্ড সংরক্ষণ;

(৭) তথ্য নিরাপত্তা ব্যবস্থার নির্দেশিকায় জন্য পরিসম্পদ ব্যবস্থাপনার নীতি অন্তর্ভুক্ত করাসহ গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে প্রবেশ ও নিগর্মন ব্যবস্থাপনার কৌশল নির্ধারণ;

(৮) নিরাপদ ইলেকট্রনিক বর্জ ব্যবস্থাপনা নিশ্চিত করা;

(৯) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর আওতাধীন সকল তথ্য পরিকাঠামোর আওতাধীন সকল তথ্য ব্যবস্থা যথাযথভাবে রক্ষণাবেক্ষণ ও হালনাগাদ করা;

(iv) পর্যবেক্ষণ বিষয়ক:

(১) বিদ্যমান তথ্য নিরাপত্তা পরিচালন পদ্ধতির (security operational process) কার্যকরতা মূল্যায়ন করা;

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

(৩) তথ্য নিরাপত্তা ব্যবস্থার নিরীক্ষা কার্য সম্পাদন করা;

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

(খ) ব্যবস্থাপনার মাধ্যমে নিয়ন্তণ:

(i) পরিসম্পদ ব্যবস্থাপনা ও উহার তালিকা প্রস্তুতকরণ:

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

(২) প্রত্যেক হার্ডওয়্যার ডিভাইস (যেমন- সার্ভার, প্রিন্টার, ল্যাপটপ, ডেস্কটপ, এক্সেস ডিভাইস, আগ্নিনির্বাপন সংক্রন্ত যন্ত্রপাতি, ইত্যাদি) ক্রমিক নম্বর সহযোগে সুস্পষ্টভাবে চিহ্নিত করা;

(৩) সফটওয়্যার এর নাম, উহার সংস্করণ, সিরিয়াল নম্বর, যে ডিভাইসের সহিত উহা সংযোজন করা হইয়াছে উহার নাম, ইত্যদির তালিকা প্রস্তুত ও নিয়মিতভাবে হালনাগাদ করা;

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

(৬) 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;

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

(ii) প্রবেশাধিকার নিয়ন্ত্রণ:

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

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নীতির আলোকে 'আবশ্যকতার ভিত্তিতে' কর্মচারী/ব্যক্তির দায়িত্ব অর্পণ করা;

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

(৪) ভূমিকা ও দায়িত্বের ভিত্তিতে ব্যক্তি/কর্মচারী চিহ্নিতক্রমে ক্ষমতা অর্পন করা;

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

(৬) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কার্য-সম্পাদনের দায়িত্বে পালনের সূত্রে যথাযথ ইউজার একাউন্ট প্রস্তুত/খোলার মাধ্যামে কম্পিউটারে সিস্টেমে প্রবেশ নিয়ন্ত্রণের কার্যকর ব্যবস্থা গ্রহণ করা;

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

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

(৯) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর প্রয়োজনীয়তার নিরিখে নিয়মিতভাবে নিরীক্ষা কার্য-সম্পাদন করা;

(১০) ডিভাইস কনফিগারেশন এ যৌক্তিক প্রবেশ কেবল এডমিনিসট্রেটর এর মধ্যে সীমাবদ্ধকরণ রাখা।

(iii) শনাক্তকরণ ও প্রমানীকরণ (authentication) নিয়ন্তণ:

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

(২) শনাক্তকরণ ও প্রমানীকরণের মাধ্যমে গুরুত্বপূর্ণ তথ্য পরিকাঠামো সহিত সম্পৃক্ত নয় এমন ব্যক্তির প্রবেশাধিকার নিয়ন্ত্রণ ব্যবস্থা পর্যালোচনা করা; এবং উক্ত পরিকাঠামোর চাকরি হইতে বরখাস্তকৃত বা চাকরি পরিত্যাগকারী ব্যক্তি/কর্মচারীর প্রবেশাধিকার নিয়ন্ত্রণ করা;

(৩) নিরাপদ পদ্ধতিতে পাসওয়ার্ড সংরক্ষণ করা;

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

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

(৬) ব্যবহারকারীর ব্যর্থ প্রচেষ্টার উপর আবশ্যিকভাবে যুক্তিসংগত ক্যাপ আরোপ করা;

(৭) ব্যবহারকারীর একাউন্টস ও প্রবেশাধিকার নিয়ন্ত্রণের কার্যকর পরীবিক্ষণ ব্যবস্থা গ্রহণ করা;

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

(iv) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর বহি:পরিসীমা (perimater) সুরক্ষা:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর বহি:পরিসীমা সুরক্ষার জন্য নীতি-কাঠামো প্রণয়ন ও উহার বাস্তবায়ন করা;

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

(৩) যথাযথ প্রবেশ নিয়ন্ত্রণ তালিকা (access control list) সহযোগে সকল অর্ন্তমূখী ও বর্হিমূখী সংযোগ ব্লক করার ব্যবস্থা করা;

(৪) প্রায়োগিকভাবে যথাযথ সুরক্ষা নীতি সহযোগে ফায়ারওয়াল ব্যবহার করা; এক্ষেত্রে অর্ন্তমূখী ও বর্হিমূখী তথ্য প্রবাহের ওয়েব কনটেণ্ট ফিল্টার এর ব্যবস্থা করা;

(৫) স্পুফকৃত ই-মেইল ব্লক করার জন্য 'সেন্ডার নীতি-কাঠামো' এর কৌশল নির্ধারণ;

(৬) "আইপি এড্রেস" এর পরিবর্তে ডোমেইন এর মাধ্যমে ওয়েবসাইটে প্রবেশের অনুমতি প্রদানের ব্যবস্থা করা;

(৭) সকল প্রবেশ পথে (gateways) ব্যবহৃত এন্টি-ভইরাস ও এন্টি-সফওয়্যার সর্বদা হালনাগাদকরণ;

(৮) নিরাপত্তা ব্যবস্থার পরিকাঠামোর সংবেদনশীল পরিবর্তনের ক্ষেত্রে 'চেইঞ্জ ম্যানেজমেন্ট প্রসেস' এর সহিত সংগতিপূর্ণ করা;

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

(১০) অভ্যন্তরীন পরিকাঠামোর অংশ বিশেষের সিস্টেম, এপ্লিকেশন, ও ডাটাবেইজের নিরাপত্তা নিশ্চিত করা;

(১১) ডিএসএ এর সার্ভার, ই-মেইল সার্ভার, বা প্রমাণীক্রত ওয়েব প্রক্সির মাধ্যমে ইন্টানেট সেবা গ্রহণের বিষয়টি পরিবীক্ষণ ও নিরীক্ষার আওতাভুক্ত করা;

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

(v) ভৌত অবকাঠামোগত ও পরিবশগত নিরাপত্তা:

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

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

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

(৪) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে অনুমোদিত ব্যক্তির প্রবেশ রোধ করিবার জন্য যথাযথ নিরাপত্তা ব্যবস্থা গড়িয়া তুলাসহ পর্য্যপ্ত সংখ্যক নিরাপত্তা কর্মী নিয়োজিত করা;

(৫) ভৌত অবকাঠামোগত ঝুঁকি মোকাবেলার জন্য গুরুত্বপূর্ণ তথ্য পরিকামোর কর্মচারীগণ দ্বারা, সময় সময়, মক্ ড্রিল সহ নিয়মিতভাবে উহা নিরীক্ষা করা;

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

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

(৮) কেবল অনুমোদিত ব্যক্তির প্রবেশ নিশ্চিত করিবার লক্ষ্যে প্রবেশ নিয়ন্ত্রণ কৌশল গড়িয়া তুলা।

(vi) হার্ডওয়্যার ও সফটওয়্যার এর পরীক্ষা মূল্যায়ন:

(১) হার্ডওয়্যার ও সফটওয়্যার এর ক্রয় ও ব্যবহারের ক্ষেত্রে মূল্যয়নের মানদন্ড নির্ধারণ করা;

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

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

(৪) শক্তিসামর্থতা (robust) রহিয়াছে এমন হার্ডওয়্যার ও সফটওয়্যার ব্যবহার করা।

(গ) পরিচালনাগত নিয়ন্ত্রণ:

(i) উপাত্ত সংরক্ষণ: হাসিং ও এনাক্রিপশন:

(১) হ্যাসিং ও এনক্রিপশনের মাধ্যমে সুরক্ষার উদ্দেশ্যে শ্রেণীবদ্ধকৃত ও সংবেদনশীল উপাত্ত চিহ্নিত করা;

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

(৩) ব্যাকআপ উপাত্তসহ সংরক্ষিত উপাত্তের হ্যাসিং ও এনক্রিপশন সম্পর্কিত নীতি-নিদের্শনার যথাযথ বাস্তবায়ন করা;

(৪) উপাত্তের হ্যাসিং ও এনক্রিপশন সংক্রান্ত নীতি-নির্দেশনার লঙ্ঘন প্রতিহত করা;

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

(ii) নিরাপত্তা বিঘ্নিত হওয়ার ঘটনা ব্যবস্থাপনা:

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

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

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

(৪) সিস্টেম সক্রিয় করিবার পূর্বে পুনরুদ্ধার এবং অরক্ষিত অবস্থা (vulnerabiity) অপসারণের ব্যবস্থা নিশ্চিত করা; এবং একবার পুনরুদ্ধার করা হইলে, নিরাপত্তা ব্যবস্থার বিঘ্নিত হইবার ঘটনা ও অবাঞ্চিত প্রবেশের চিহ্ন মুছে ফেলা ও উহার বিশ্লেষণ করা;

(৫) ভবিষ্যতে নিরাপত্তা বিঘ্নিত হইবার ঘটনা প্রতিরোধের উদ্দেশে উক্তরূপ ঘটনা বিশ্লেষণের পর এতদবিষয়ের সুপারিশসমূহ ব্যবস্থাপনা কর্তৃপক্ষের নিকট উপস্থাপন করা।

(iii) দক্ষতা উন্নয়ন, প্রশিক্ষণ, ইত্যদি:

(১) প্রশিক্ষণের কৌশল, পরিকল্পনা ও কর্মসূচী পর্য্যলোচনা করা;

(২) অরক্ষিত অবস্থা ও নিরাপত্তা ঝুঁকি চিহ্নিতকরণ ও মূল্যায়ন;

(৩) দক্ষতা উন্নয়ন কর্মসূচী ও প্রশিক্ষণ ব্যবস্থার মূল্যয়ন করা;

(৪) দক্ষতা উন্নয়নের প্রয়োজনীয়তা নিরূপন ও উহার বাস্তবায়ন;

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

(iv) উপাত্তের ক্ষতি প্রতিরোধ (data loss prevention):

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

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

(৩) ট্রেকিং এর মাধ্যমে অননুমোদিত উপাত্ত প্রবাহ পরিবীক্ষণের জন্য নেটওয়ার্ক মনিটরিং টুলস ব্যবহার করা;

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

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

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

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

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

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

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

(১২) প্রান্তসীমা (end point) সুরক্ষা ব্যবস্থার মাধ্যমে কর্মক্ষেত্রের কম্পিউটার নিয়ন্ত্রণ করা।

(v) পেনিট্রেশন টেস্টিং:

[প্রয়োজনীয় কনটেন্ট এর ভিত্তিতে পরে যোগ করা হবে]

(vi) নেটওয়ার্ক ডিভাইস সুরক্ষা:

(১) বলিষ্ঠ পাসওয়ার্ড ব্যবহার করা;

(২) নির্দ্দিষ্ট সময় অন্তর পাসওয়ার্ড পরিবর্তন করা;

(৩) নিরাপত্তা ব্যবস্থার নীতি অনুসরণে প্রবেশাধিকার নিয়ন্ত্রণ করা;

(৪) অন্তর্মূখী ও বর্হিমূখী তথ্য প্রবাহ পরিবীক্ষণ ও বিশ্লেষণ করা;

(৫) নিরাপত্তা ব্যবস্থার সহিত সামন্জস্যহীন অংশ হালনাগাদ করা;

(৬) নেটওয়ার্ক টপোলজি ও আর্কিটেকচার সমন্বয় করা।

(vii) গুরুত্বপূর্ণ তথ্য হস্তান্তর ও স্থানান্তর:

[প্রয়োজনীয় কনটেন্ট এর ভিত্তিতে পরে যোগ করা হবে]

(এ) ইন্ট্রানেট এর নিরাপত্তা ব্যবস্থাপনা:

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

(২) 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;

(৩) 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;

(৪) পাবলিক নেটওয়ার্ক হইতে ইন্ট্রানেট সম্পূর্ণভাবে বিছিন্ন রাখা;

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

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

(৭) নির্দিষ্ট সময় অন্তর ইন্ট্রানেট নেটওয়ার্ক নিরীক্ষা করা;

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

(৯) ক্ষতিকর তথ্য প্রবাহ (যেমন- স্পাম, ফিসিং, সাইওয়্যার, এডওয়্যার, ম্যালওয়্যার, ইত্যাদি) ব্লক বা ট্র্যাক করিবার জন্য ইন্ট্রানেট এ ই-মেইল ফিল্টার রাখা;

(১১) ইন্ট্রানেট এ রক্ষিত গোপনীয় তথ্য ব্যবস্থায় ক্ষতিকর হামলাকারীর অননুমোদিত প্রবেশ রোধ করিবার জন্য সিকিউর সকেট লেয়্যার ডিজিটাল সনদের ব্যবহার করা।

(viii) প্রাগ্রসর পুন: হন: হামলার ঘটনার সুরক্ষা:

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

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

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

(৪) কম্পিউটার ব্যবস্থায় অবাঞ্চিত প্রবেশ রোধের ক্ষেত্রে নিয়মিতভাবে হালনাদাদকৃত ম্যালওয়্যার সুরক্ষার ব্যবস্থাসহ প্যাচ, ভার্ষণ প্যাক, হট বক্স, ইত্যাদির দ্রুত প্রয়োগ ব্যবস্থার উন্নয়ন করা;

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

(ix) উপাত্ত ব্যাক-আপ ও পুনরুদ্ধার পরিকল্পনা:

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

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

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

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

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

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

(x) নিরাপদ ও সহিষ্ণু নকশা (architecture) বিস্তারণ (deployment):

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

(২) নেটওয়ার্ক নকশায় নিরাপত্তার ব্যবস্থাকে একট গুরুত্বপূর্ণ উপাদান হিসেবে সংযুক্ত করা;

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

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

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

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

(৭) অটোমেটেড আপগ্রেডস ও লগ মনিটরিং ব্যবস্থা নিরপত্তা ব্যবস্থার নকশা বিস্তারণের অংশ করা;

(৮) 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;

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

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

(xi) নিরাপত্তা ব্যবস্থার হুমকি সংক্রান্ত বিষয়ের রিপোর্টিং:

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

(২) এজেন্সির নিকট হইতে, সময় সময়, প্রাপ্ত গোপনীয় তথ্যাদি যাহাতে যাহাতে প্রকাশ না পায় সেইজন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে কর্মচারীগণের সহিত নন-ডিসক্লোজার চুক্তি সম্পাদন করা;

(৩) এজেন্সির কর্তক, সময় সময়, আয়োজিত কর্মশালা, সেমিনার প্রশিক্ষন কর্মসূচীতে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কর্মকর্তা ও কর্মচারীদের অংশগ্রহণের ব্যবস্থা করা;

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

(৫) মোক্ ড্রিল, পেনিট্রেশন টেস্টিং সংক্রান্ত পরামর্শ বাস্তবায়ন সংক্রন্ত তথ্য যথাবিহিতভাবে এজেন্সিকে অবহিত করা; এবং উক্তরূপ গুরুত্বপূর্ণ তথ্য সম্পর্কে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ফিডব্যাক চ্যানেলের মাধ্যমে সরকার/এজিন্সিকে রিপোর্ট করা;

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

(xii) নিরীক্ষা এবং আক্রম্যতা (vulneralibity) নিরুপণ:

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

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

(৩) আক্রম্যতা বিষয়ে প্রশিক্ষণ প্রদান, সচেতনতা বৃদ্ধি, নিরীক্ষা, ইত্যাদির মাধ্যামে ডিজিটাল নিরাপত্তা ব্যবস্থার প্রয়োগিক ব্যবস্থা গ্রহণ করা;

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

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

(xiii) ডিজিটাল নিরাপত্তা সংক্রান্ত সুপারিশ বাস্তবায়ন:

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামোতে ডিজিটাল নিরাপত্তা ব্যবস্থা সংক্রান্ত্র সুপারিশ বাস্তবায়নের জন্য একটি ‘কমপ্লায়েন্স কমিটি’ গঠন করা;

(২) ডিজিটাল নিরাপত্তা ব্যবস্থার সংক্রান্ত সুপারিশ বাস্তবায়নের বিষয়ে রিপোর্ট প্রণয়েনর জন্য কৌশল প্রণয়ন করা;

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

(৪) ডিজিটাল নিরাপত্তা ব্যবস্থার সুপারিশ বাস্তবায়ন না করিবার ক্ষেত্রে প্রয়োজনীয় অনুসন্ধান তদন্তের ব্যবস্থা করা;

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

(৬) নিয়ম-নীতি লঙ্ঘন বিষয়ে তাৎক্ষণিকভাবে রিপোর্ট প্রদানক্রমে উক্ত বিষয়ে যথাযথ ব্যবস্থা গ্রহণ করা।

অংশ-১২

গুরুত্বপূর্ণ তথ্য পরিকাঠামো চিহ্নিতকরণ

২৪। গুরুত্বপূর্ণ তথ্য পরিকাঠামো চিহ্নিতকরণে অনুসরণীয় নীতি।- (১) গুরুত্বপূর্ণ তথ্য পরিকাঠামো হিসেবে চিহ্নিত করা হইবে এমন সকল সংস্থা ব প্রতিষ্ঠানের কার্যাবলী ও প্রদত্ত সেবার সংবেদনশীলতা এবং উক্ত সংস্থা বা প্রতিষ্ঠানের তথ্য ও যোগাযোগ প্রযুক্তি কাঠামো অসমর্থ হইবার ক্ষেত্রে জাতীয় নিরাপত্তা, অর্থনীতি, জনস্বাস্থ্য বা জননিরাপত্তার উপর উহার প্রভাব বিবেচনাক্রমে নিম্নবর্ণিত বৈশিষ্টের ভিত্তিতে নিরূপণ করা যাইবে-

(ক) নিম্নবর্ণিত তথ্যের ভিত্তিতে ভোক্তা ও সরকারী কর্মকান্ডের উপর প্রভাব নিরূপণের করিতে হইবে-

(অ) প্রতিদিনের লেনদেনের মোট সংখ্যা;

(আ) প্রতিদিনের সকল ধরনের লেনদেনের মোট মূল্য;

(ই) সংযুক্ত যন্ত্রপাতির (device) সংখ্যা ও নেটওয়ার্ক সাইজ;

(ঈ) বিভিন্ন শ্রেনীর ভোক্তার সংখ্যা;

(খ) ব্যবহারিক সময় কাঠামো (ঘন্টা, দিন, সপ্তাহ);

(গ) তথ্য ও যোগাযোগ প্রযুক্তি কাঠামোর অসামর্থতার ক্ষেত্রে ভৌগলিক বা পরিবশগত প্রভাব, যদি থাকে;

(ঘ) তথ্য ও যোগাযোগ প্রযুক্তি কাঠামো অসামর্থতা বা বিনষ্টের কারণে সেবা প্রাপ্তির অ-লভ্যতার উপর সামগ্রিক প্রভাব;

(ঙ) অন্যান্য সংবেদনশীল খাতে প্রদেয় অপরিহার্য সেবার উপর নির্ভরশীলতা।

২৫। গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সুরক্ষার ক্ষেত্রে এজেন্সি কর্তৃক অনুসরণীয় নীতি।- গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সুরক্ষার ক্ষেত্রে এজেন্সি নিম্নবর্ণিত নীতি-নির্দেশনা অনুসরণ করিবে, যথা:-

(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামো চিহ্নিতকরণে কার্য-পদ্ধতির উন্নয়ন করা;

(২) ডিজিটাল নিরাপত্তা ঝুঁকি ব্যবস্থাপনার মাধ্যমে গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সুরক্ষা নিশ্চত করা;

(৩) গুরুত্বপূর্ণ তথ্য পরিকাঠামো কর্তৃক এতদবিষয়ে এজন্সি কর্তৃক জারীকৃত নীতি, গাইডলাইন, পরামর্শ ও সতর্কতা, ইতাদির প্রয়োগ নিশ্চিত করা;

(৪) রিয়েল টাইম ওয়ানিং সিস্টেম এর সক্ষমতা বৃদ্ধি করা;

(৫) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সহিত ডিজিটাল নিরাপত্তা ঝুঁকি, হামলা, আক্রম্যতা ও এতদসংক্রন্ত বিষয়ের উপর তথ্য বিনিময়ের সুযোগ-সুবিধা বৃদ্ধি করা;

(৬) গুরুত্বপূর্ণ তথ্য পরিকাঠামো সংক্রান্ত গৃহীত জাতীয় নীতি ও কর্মসূচী সমন্বয় করা;

(৭) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সুরক্ষা সম্পর্কিত গবেষণা ও উন্নয়নে উৎসাহদান করা;

(৮) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সুরক্ষা নিশ্চিত করিবার জন্য জাতীয় ও আন্তজার্তিক পর্যায়ে যোগাযোগ স্থাপন করা;

(৯) ডিজিটাল নিরাপত্তা বিঘ্নিত হওয়ার ঘটনা, হুমকি, হামলা, গুপ্তচরবৃত্তি, ইত্যাদি সম্পর্কে গুরুত্বর্পণ তথ্য বিনিময় ব্যবস্থা প্রবর্তন করা;

(১০) ডিজিটাল নিরাপত্তা সংক্রান্ত বিষয়ে সচেতনতা সৃষ্টির লক্ষে সেমিনার, সিম্পোজিয়াম, ক্বর্মশালা আয়োজন ও পরিচালনা করা;

(১১) দক্ষ জনবল সৃষ্টির লক্ষ্যে সক্ষমতা তৈরীর কর্মসূচি গ্রহণ করা;

(১২) সংবেদনশীল খাত ভিত্তিক ক্রিটিকাল ইমারজেন্সি রেসপন্স টীম প্রতিষ্ঠার পদক্ষেপ গ্রহণ করা।

অংশ-১৩

বিবিধ

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

২৭। নির্দেশ প্রদানের ক্ষমতা।- কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামো এই গাইডলাইনে বিধৃত বিধানাবলি প্রতিপালনে অসমর্থ হইলে, মহাপরিচালক, লিখিতভাবে, উক্ত বিধানাবলি অনুসরণের জন্য নির্দেশ প্রদান করিতে পারিবে; এবং উক্তরূপে কোনো নির্দেশ প্রদান করা হইলে সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো উহা প্রতিপালনে বাধ্য থাকিবে।

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

( )

মহাপরিচালক

ডিজিটাল নিরাপত্তা এজেন্সি।