রেজিস্টার্ড নং ডি এ-১

বাংলাদেশ গেজেট

অতিরিক্ত সংখ্যা

কর্তৃপক্ষ কর্তৃক প্রকাশিত

রবিবার, মার্চ ৮, ২০২০

গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ডাক, টেলিযোগাযোগ এবং তথ্য প্রযুক্তি মন্ত্রণালয়

প্রজ্ঞাপন

তারিখ : ১১ ফাল্গুন, ১৪২৬ বঙ্গাব্দ/২৪ ফেব্রুয়ারি, ২০২০ খ্রিস্টাব্দ।

এস. আর. ও নং ৬০-আইন/২০২০।—ডিজিটাল নিরাপত্তা আইন, ২০১৮ (২০১৮ সনের ৪৬ নং আইন) এর ধারা ৬০ এ প্রদত্ত ক্ষমতাবলে সরকার নিম্নরূপ বিধিমালা প্রণয়ন করিল, যথা :—

১। **সংক্ষিপ্ত শিরোনাম।**—এই বিধিমালা ডিজিটাল নিরাপত্তা বিধিমালা, ২০২০ নামে অভিহিত হইবে।

২। **সংজ্ঞা।**—(১) বিষয় বা প্রসঙ্গের পরিপন্থী কোনো কিছু না থাকিলে, এই বিধিমালায়—

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

(খ) ‘ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনা’ অর্থ প্রকৃত বা সম্ভাব্য ডিজিটাল নিরাপত্তা সংক্রান্ত এমন বৈরী পরিস্থিতির উদ্ভব হয় যাহার ফলে ডিজিটাল নিরাপত্তা ব্যবস্থা ও এতদ্‌সংক্রান্ত নীতিমালা লঙ্ঘনক্রমে কোনো কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার রিসোর্স নেটওয়ার্ক বা অন্য কোনো ডিভাইসে অননুমোদিত প্রবেশ সংঘটিত হয় বা উক্তরূপ অননুমোদিত প্রবেশের ফলে সেবা প্রদান বন্ধ বা ব্যাহত হয় বা কম্পিউটার, কম্পিউটার সিস্টেম, কম্পিউটার রিসোর্স নেটওয়ার্ক বা অন্য কোনো ডিভাইস অননুমোদিত ব্যবহারের মাধ্যমে কোনো তথ্যের পরিবর্তন বা তথ্য উপাত্ত প্রক্রিয়াকরণ বা এইরূপ ঘটনা সংঘঠিত হয়;

মূল্য : টাকা ২৪.০০

(গ) ‘তথ্যপ্রযুক্তি নিরীক্ষা’ বা ‘ফরেনসিক ল্যাব নিরীক্ষা’ অর্থ ডিজিটাল নিরাপত্তা এজেন্সি কর্তৃক স্বীকৃত এবং আন্তর্জাতিকভাবে সর্বজনগ্রাহ্য (accredited) পদ্ধতিতে তথ্য প্রযুক্তি নিরাপত্তা বিষয়ে কর্মসম্পাদন করিয়া থাকেন এইরূপ ব্যক্তি বা প্রতিষ্ঠান কর্তৃক কোনো প্রতিষ্ঠানের তথ্য প্রযুক্তি অবকাঠামো এবং এতদ্‌উদ্দেশ্যে প্রণীত নীতির অধীন কৃত কার্যক্রমের পরীক্ষা এবং মূল্যায়ন;

(ঘ) ‘তফসিল’ অর্থ এই বিধিমালার সহিত সংযোজিত তফসিল;

(ঙ) ‘স্বীকৃত’; অর্থ এজেন্সি কর্তৃক স্বীকৃত।

(২) এই বিধিমালায় ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞা এই বিধিমালায় প্রদান করা হয় নাই, সেই সকল শব্দ বা অভিব্যক্তি আইন বা তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ (২০০৬ সনের ৩৯ নং আইন) এ যেই অর্থে ব্যবহৃত হইয়াছে সেই অর্থে ব্যবহৃত হইবে।

৩। **ডিজিটাল নিরাপত্তা এজেন্সির ক্ষমতা।**—আইনের ধারা ৫ এর উদ্দেশ্য পূরণকল্পে, ডিজিটাল নিরাপত্তা এজেন্সির ক্ষমতা হইবে নিম্নরূপ, যথা :—

(ক) তথ্য প্রযুক্তি সংক্রান্ত রাষ্ট্রীয় সংকট মোকাবেলার নিমিত্ত সংশ্লিষ্ট সরকারি ও বেসরকারি সংস্থা ও প্রতিষ্ঠানের সহিত সমন্বয় সাধন ও তৎসম্পর্কে প্রয়োজনীয় নির্দেশনা প্রদান;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো, ফরেনসিক ল্যাব ও তথ্যপ্রযুক্তির নিরীক্ষার গাইডলাইন প্রণয়ন এবং তদানুসারে নিরীক্ষা;

(গ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর—

(অ) নিরাপত্তা নিশ্চিতকরণের প্রয়োজনীয় ব্যবস্থা গ্রহণ এবং যথাযথ ক্ষেত্রে, পরিদর্শনপূর্বক উহা সংশোধনের প্রয়োজনীয় নির্দেশনা প্রদান;

(আ) ঝুঁকি হ্রাস ও সামগ্রিক নিরপত্তা নিশ্চিতকল্পে, যথাযথ কর্মকৌশল প্রণয়ন ও উহার বাস্তবায়ন পরিবীক্ষণ ও পরিদর্শনের কার্যপদ্ধতি নির্ধারণ;

(ই) পরিচালনা পদ্ধতি ও রক্ষণাবেক্ষণ মানদণ্ড প্রণয়ন এবং উক্ত পরিকাঠামোতে নিয়োজিত ব্যক্তির জন্য অনুসরণীয় কার্যপদ্ধতি নির্ধারণ;

(ঘ) ডিজিটাল ফরেনসিক ল্যাব স্থাপন, পরিচালন, রক্ষণাবেক্ষণ ও নিয়ন্ত্রণ;

(ঙ) ডিজিটাল নিরাপত্তায় ব্যবহৃত কম্পিউটারের হার্ডওয়্যার ও সফটওয়্যারের মানসহ উক্তরূপ নিরাপত্তার কার্যে ব্যবহৃত সেবা ও পণ্যের মান নির্ধারণ;

(চ) ডিজিটাল নিরাপত্তার সহিত নিয়োজিত জনবলের দক্ষতার মান নির্ধারণ এবং কম্পিউটার ও কম্পিউটার সিস্টেমের নিরাপত্তা তদারকি ও এতদ্‌সংক্রান্ত সক্ষমতা বৃদ্ধিকরণ;

(ছ) ডিজিটাল নিরাপত্তা সেবার উন্নয়ন এবং দক্ষ পরিচালনার জন্য প্রয়োজনীয় অন্য কোনো পদক্ষেপ গ্রহণ।

৪। **ডিজিটাল নিরাপত্তা এজেন্সির দায়িত্ব ও কার্যাবলি।**—আইনের ধারা ৫ এর উদ্দেশ্যে পূরণকল্পে, ডিজিটাল নিরাপত্তা এজেন্সির দায়িত্ব ও কার্যাবলি হইবে নিম্নরূপ, যথা :—

(ক) দেশে ডিজিটাল ডিভাইস এবং তথ্য ও যোগাযোগ প্রযুক্তি ব্যবহারের মাধ্যমে সংঘটিত অপরাধ দমন সংক্রান্ত কার্যক্রমের সমন্বয়;

(খ) ডিজিটাল নিরাপত্তা সেবার ব্যবস্থা প্রবর্তন এবং উহার পরিচালন, রক্ষণাবেক্ষণ, পরিবীক্ষণ ও নিয়ন্ত্রণ এবং ডিজিটাল নিরাপত্তা সেবা প্রদান নিশ্চিত করিবার লক্ষ্যে উক্ত সেবা প্রদানকারীগণের মধ্যে পারস্পরিক সহযোগিতামূলক পরিস্থিতি বজায় রাখা ও উহাতে উৎসাহ প্রদান;

(গ) ডিজিটাল নিরাপত্তা সংক্রান্ত গবেষণা কার্যক্রম গ্রহণ ও উহার সার্বিক উন্নয়নে সহায়তা প্রদান;

(ঘ) বিভিন্ন বিশ্ববিদ্যালয় ও গবেষণা প্রতিষ্ঠানের সহিত জাতীয় অর্থনীতির বিভিন্ন খাতে তথ্য ও যোগাযোগ প্রযুক্তির নিরাপত্তা নিশ্চিতকরণ;

(ঙ) এজেন্সি কর্তৃক নির্ধারিত মান অনুসারে ডিজিটাল নিরাপত্তা সেবা প্রদান করা হইতেছে কিনা উহা পরিবীক্ষণের ব্যবস্থা গ্রহণ;

(চ) ডিজিটাল নিরাপত্তা বিষয়ক অভ্যন্তরীণ ও আন্তর্জাতিক হুমকির উৎস পর্যবেক্ষণ এবং উক্ত বিষয়ে সংশ্লিষ্ট সকলকে সতর্কীকরণ ও প্রতিকারমূলক ব্যবস্থা গ্রহণ;

(ছ) জাতীয় নিরাপত্তা, বহিঃসম্পর্ক, জনস্বাস্থ্য, জনশৃঙ্খলা বা প্রয়োজনীয় ও অপরিহার্য সেবার ক্ষেত্রে ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার হুমকি পরিলক্ষিত হইলে প্রতিকারের সক্রিয় ব্যবস্থা গ্রহণ;

(জ) ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনা (incident) সম্পর্কে অন্যান্য রাষ্ট্রের অনুরূপ কর্তৃপক্ষের সহিত পারস্পারিক সহযোগিতা বিনিময়;

(ঝ) ডিজিটাল নিরাপত্তা সেবা প্রদান সংক্রান্ত শিল্পের প্রসার ও উন্নয়নের বিষয়ে প্রয়োজনীয় পদক্ষেপ গ্রহণ এবং উক্ত শিল্পে জড়িত ব্যক্তির দক্ষতা ও পেশাগত মান উন্নয়নে প্রয়োজনীয় সহায়তা প্রদান;

(ঞ) বাংলাদেশ ও বর্হিবিশ্ব হইতে ডিজিটাল নিরাপত্তা সংক্রান্ত তথ্য সংগ্রহক্রমে বাংলাদেশে উহার প্রভাব সম্পর্কে পর্যালোচনা করা ও তদানুসারে প্রয়োজনীয় ব্যবস্থা গ্রহণের বিষয়ে সরকারের নিকট সুপারিশ প্রেরণ;

(ট) ডিজিটাল নিরাপত্তা সংক্রান্ত বিভিন্ন প্রশিক্ষণ, কর্মশালা ও সেমিনারের আয়োজনসহ জনসচেতনতামূলক কার্যক্রম গ্রহণ;

(ঠ) ডিজিটাল নিরাপত্তার দুর্বলতা, ডিজিটাল নিরাপত্তা লঙ্ঘন ও ক্ষতিকারক ক্রিয়াকলাপ সম্পর্কে অনুসন্ধান;

(ড) ডিজিটাল নিরাপত্তার ক্ষেত্রে আন্তর্জাতিক প্রতিষ্ঠান ও বিদেশী সরকারের সহিত, সরকারের পূর্বানুমোদনক্রমে, চুক্তি সম্পাদন, তথ্য বিনিময় ও সহযোগিতা করা;

(ঢ) এজেন্সির কর্মকর্তা-কর্মচারীগণকে ডিজিটাল নিরাপত্তা বিষয়ে প্রশিক্ষণ প্রদান;

(ণ) সরকারের পূর্বানুমোদনক্রমে ডিজিটাল নিরাপত্তা সংক্রান্ত আন্তর্জাতিক পরিমণ্ডলে সরকারের প্রতিনিধিত্ব করা;

(ত) জাতীয় ডিজিটাল নিরাপত্তা সংক্রান্ত বিষয়ে নীতিমালা প্রণয়নের ব্যাপারে সরকারকে পরামর্শ প্রদান।

৫। **মহাপরিচালকের ক্ষমতা ও দায়িত্ব।**—আইনের ধারা ৬ এর উপ-ধারা (২) এর উদ্দেশ্য পূরণকল্পে, মহাপরিচালক, অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত কার্য-সম্পাদন করিবেন, যথা :—

(ক) তথ্য ও যোগাযোগ প্রযুক্তিভিত্তিক হুমকি মোকাবেলায় প্রয়োজনীয় ব্যবস্থা গ্রহণ;

(খ) বিভিন্ন সংস্থা ও প্রতিষ্ঠানের ডিজিটাল নিরাপত্তা সংক্রান্ত কার্যক্রমের বিষয়ে পরামর্শ প্রদান বা, ক্ষেত্রমত, নির্দেশনা প্রদান;

(গ) দেশের ডিজিটাল নিরাপত্তা ব্যবস্থার তদারকি;

(ঘ) কম্পিউটার ইমার্জেন্সি রেসপন্স টিমসমূহের মধ্যে সমন্বয়সাধন ও তত্ত্বাবধান;

(ঙ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো ঘোষণার বিষয়ে সরকারকে পরামর্শ প্রদান এবং আইনের ধারা ১৬ এর উদ্দেশ্য পূরণকল্পে, উক্ত পরিকাঠামো পরিবীক্ষণ ও পরিদর্শনক্রমে উক্ত বিষয়ে প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য সরকারের নিকট প্রতিবেদন উপস্থাপন;

(চ) সরকারের পূর্বানুমোদনক্রমে, নিম্নবর্ণিত বিষয়ে নীতিমালা প্রণয়ন এবং প্রয়োজনীয় ক্ষেত্রে নির্দেশনা জারিকরণ, যথা :—

(অ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো চিহ্নিতকরণ;

(আ) তথ্য নিরাপত্তার বিধি-বিধান অনুসরণসহ সংরক্ষিত ব্যবস্থার পদ্ধতি নির্ধারণ;

(ই) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সুরক্ষা প্রদান;

(ঈ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা মূল্যায়নের লক্ষ্যে প্রয়োজনীয় তথ্য উপাত্ত সংগ্রহ এবং উহাদের প্রতিকারমূলক ব্যবস্থা;

(উ) সরকারি-বেসরকারি অংশগ্রহণ, ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার হুমকি সনাক্তকরণ এবং সংরক্ষিত ব্যবস্থার মানদণ্ড নির্ধারণ।

৬। **জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিমের দায়িত্ব ও কার্যাবলি।**—জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম, আইনের ধারা ৯ এর উপ-ধারা (৪) এ বর্ণিত দায়িত্বের অতিরিক্ত অন্যান্য বিষয়ের মধ্যে, নিম্নবর্ণিত দায়িত্ব পালন ও কার্য-সম্পাদন করিবে, যথা :—

(ক) ডিজিটাল আক্রমণ ও হুমকির ঘটনা রোধের সময়োচিত ও প্রয়োজনীয় কার্যক্রম গ্রহণ এবং প্রয়োজনীয়তার নিরিখে অন্যান্য গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও সংশ্লিষ্ট অংশীজনের সহিত সমন্বয় সাধন;

(খ) ডিজিটাল আক্রমণ ও হুমকির ঘটনার শ্রেণিবিভাগ ও সত্যতা যাচাই, এবং সম্ভাব্য ডিজিটাল আক্রমণ ও হুমকি সম্পর্কে অগ্রাধিকার ভিত্তিতে করণীয় নির্ধারণ;

(গ) ডিজিটাল নিরাপত্তা সংক্রান্ত হুমকি বা ঝুঁকি বিষয়ে গুরুত্বপূর্ণ তথ্য পরিকাঠামো সংশ্লিষ্ট কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও সংশ্লিষ্ট অংশীজনের নিকট হইতে তথ্য সংগ্রহ ও উক্ত বিষয়ে সতর্কীকরণ তথ্য প্রেরণ ;

(ঘ) আইনের অধীন অপরাধ সংঘটনের ঘটনা সম্পর্কে তথ্য সংগ্রহ ;

(ঙ) ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনা নিষ্পত্তির লক্ষ্যে সংশ্লিষ্ট কম্পিউটার ইমার্জেন্সি রেসপন্স টিমসমূহের মধ্যে সমন্বয়সাধন এবং উহাদের এতদ্‌সংক্রান্ত কার্যক্রমের অগ্রগতি পর্যবেক্ষণ;

(চ) কম্পিউটার ইমাজেন্সি রেসপন্স টিম ও সংশ্লিষ্ট ব্যক্তি ও প্রতিষ্ঠানের সহিত যোগাযোগ নেটওয়ার্ক প্রতিষ্ঠা;

(ছ) ডিজিটাল নিরাপত্তা সেবা প্রদান সংক্রান্ত কমিউনিটি গ্রুপ গঠন, উক্ত বিষয়ে গবেষণা ও উন্নয়ন কর্মকাণ্ডে জড়িত প্রতিষ্ঠান চিহ্নিতকরণ;

(জ) সরকারের পূর্বানুমোদনক্রমে, সংশ্লিষ্ট দেশসমূহের জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিমসমূহকে, প্রযোজ্য ক্ষেত্রে অন্যান্য দেশের সহিত সম্পাদিত চুক্তির অধীন প্রয়োজনীয় তথ্য প্রেরণ ও পারস্পরিক সহযোগিতা বিনিময়;

(ঝ) ডিজিটাল নিরাপত্তা সম্পর্কিত ঘটনা মোকাবেলা এবং তৎসংক্রান্ত ঘটনার পূর্বাভাস প্রদান ও উহা প্রতিরোধকরণ;

(ঞ) ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনার ফরেনসিক বিশ্লেষণ;

(ট) ডিজিটাল নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে প্রয়োজনীয় তথ্য প্রযুক্তি নিরীক্ষা কার্যক্রম সম্পাদন এবং ডিজিটাল নিরাপত্তার দুর্বলতা, উহার লঙ্ঘন এবং ক্ষতিকারক কর্মকাণ্ড ও উৎস অনুসন্ধান;

(ঠ) ডিজিটাল নিরাপত্তা সংক্রান্ত বিষয়ে সংশ্লিষ্ট কর্মকর্তা ও কর্মচারীগণকে প্রশিক্ষণ ও প্রযুক্তিগত পরামর্শ প্রদান।

৭। **ডিজিটাল নিরাপত্তা সংক্রান্ত তথ্যপ্রেরণ, ইত্যাদি**।—(১) কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা কোনো ব্যক্তি, প্রতিষ্ঠান বা ডিজিটাল রিসোর্স এর ডিজিটাল নিরাপত্তা বিঘ্নিত হইলে বা ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা ঘটিলে বা তথ্য পরিকাঠামো নিয়ন্ত্রণাধীন কম্পিউটার বা কম্পিউটার সিস্টেমের নিরাপত্তা বিঘ্নিত হইবার ঘটনা বা অন্য কোনো ঘটনা ঘটিলে, সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা ব্যক্তি, প্রতিষ্ঠান বা ডিজিটাল রিসোর্স এজেন্সি কর্তৃক নির্ধারিত সময়, ছক ও পদ্ধতিতে, যদি থাকে, উক্ত তথ্য জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিমের নিকট প্রেরণ করিবে।

(২) জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম, প্রয়োজনে, স্বীয় উদ্যোগে, উপ-বিধি (১) এ উল্লিখিত বিষয়ে গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা কোনো ব্যক্তি, প্রতিষ্ঠান বা ডিজিটাল রিসোর্স হইতে, সময় সময় এজেন্সি কর্তৃক নির্ধারিত ছকে ও পদ্ধতিতে, প্রয়োজনীয় তথ্য প্রেরণের জন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা কোনো ব্যক্তি, প্রতিষ্ঠান বা ডিজিটাল রিসোর্স এর সংশ্লিষ্ট দায়িত্বপূর্ণ ব্যক্তিকে অনুরোধ জানাইতে পারিবে; এবং উক্ত রূপে কোনো তথ্য প্রেরণের জন্য অনুরোধ করা হইলে সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা কোনো ব্যক্তি, প্রতিষ্ঠান বা ডিজিটাল রিসোর্স এর দায়িত্বপূর্ণ ব্যক্তি উহা সরবরাহ বা প্রেরণ করিতে বাধ্য থাকিবেন।

(৩) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা কোনো ব্যক্তি, প্রতিষ্ঠান বা ডিজিটাল রিসোর্স উহার ডিজিটাল নিরাপত্তা বিঘ্ন হইবার ঝুঁকি বা ডিজিটাল নিরাপত্তা বিঘ্নিত হইবার ঘটনা চিহ্নিতকরণের জন্য প্রয়োজনীয় উদ্যোগ গ্রহণ করিবে।

(৪) জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম, উপবিধি (১) ও (২) এর অধীন প্রাপ্ত তথ্য—

(ক) এজেন্সি কর্তৃক নির্ধারিত পদ্ধতিতে সংরক্ষণ এবং উক্ত তথ্যের গোপনীয়তা রক্ষার যুক্তিসংগত পদক্ষেপ গ্রহণ করিবে;

(খ) সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামো বা ব্যক্তি, প্রতিষ্ঠান বা ডিজিটাল রিসোর্স এর লিখিত অনুমতি ব্যতিরেকে, প্রকাশ করিতে পারিবে না।

(৫) উপবিধি (৪) এ যাহা কিছুই থাকুক না কেন, জাতীয় ইমার্জেন্সি রেসপন্স টিম ডিজিটাল নিরাপত্তা হুমকি মোকাবেলা ও জনসচেতনতা সৃষ্টির লক্ষ্যে, এজেন্সি কর্তৃক নির্ধারিত পদ্ধতিতে, উক্তরূপ হুমকির বিদ্যমান প্রবণতা সংক্রান্ত তথ্য সর্বসাধারণের অবগতির জন্য প্রকাশ করিতে পারিবে।

(৬) এজেন্সি জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও অন্যান্য কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এবং সংশ্লিষ্ট সেবা প্রদানকারী, ডাটা সেন্টার ও অন্যান্য প্রতিষ্ঠানের মধ্যে তথ্য বিনিময় সংক্রান্ত যাবতীয় যোগাযোগসহ অন্যান্য কর্মকাণ্ড দ্রুত, সুষ্ঠু ও দক্ষতার সহিত সম্পন্নের জন্য জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এবং অন্যান্য কম্পিউটার ইমার্জেন্সি রেসপন্স টিমসহ সংশ্লিষ্ট সকল প্রতিষ্ঠানের ফোকাল পয়েন্ট নির্ধারণের ব্যাপারে প্রয়োজনীয় ব্যবস্থা গ্রহণ করিতে পারিবে এবং উক্তরূপ যোগাযোগ সম্পর্কিত যাবতীয় তথ্য ওয়েব সাইটে প্রকাশের ব্যবস্থা গ্রহণ করিবে।

৮। **জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এর কার্যালয়**।—(১) জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ডিজিটাল নিরাপত্তা এজেন্সির প্রশাসনের অংশ হিসেবে পরিগণিত হইবে এবং উহার নিয়ন্ত্রণাধীন একটি প্রতিষ্ঠান হিসেবে উহার কার্য-সম্পাদন করিবে।

(২) এজেন্সির প্রশাসনিক কার্যালয় বা এজেন্সি কর্তৃক নির্ধারিত অন্য কোনো স্থানে জাতীয় কম্পিউটার এমার্জেন্সি রেসপন্স টিমের কার্যালয় থাকিবে।

৯। **জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম এর সার্বক্ষণিক দায়িত্ব**।—(১) জাতীয় কম্পিউটার এমার্জেন্সি রেসপন্স টিম, সমগ্র বৎসর ২৪ (চব্বিশ) ঘণ্টার ভিত্তিতে, সরকারি ও অন্যান্য ছুটির দিনসহ, সার্বক্ষণিকভাবে উহার দায়িত্ব পালন করিবে।

(২) উক্ত টিমের সহিত যোগাযোগের ঠিকানা এজেন্সির ওয়েবসাইটে প্রকাশ করা হইবে।

১০। **তথ্য বিনিময়**।—জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ডিজিটাল নিরাপত্তা সংক্রান্ত বিষয়ে তথ্য বিনিময় ও তথ্য প্রচার করিবার উদ্দেশ্যে নিম্নবর্ণিত ব্যক্তি, সংস্থা বা প্রতিষ্ঠানের সহিত মতবিনিময় ও প্রয়োজনীয় সহায়তা প্রদান করিতে ও উক্ত ব্যক্তি, সংস্থা ও প্রতিষ্ঠানের সহযোগিতা গ্রহণ করিতে পারিবে, যথা :—

(ক) দেশের অভ্যন্তরীণ অন্যান্য কম্পিউটার ইমার্জেন্সি রেসপন্স টিম;

(খ) ডিজিটাল নিরাপত্তা প্রদানের সহিত সংশ্লিষ্ট প্রতিষ্ঠান;

(গ) ইন্টারনেট রেজিস্ট্রি এবং ডোমেইন রেজিস্টার্স;

(ঘ) আইসিটি শিল্প;

(ঙ) ডিজিটাল নিরাপত্তার সহিত সংশ্লিষ্ট পণ্য ও সেবা প্রদানকারী প্রতিষ্ঠানসমূহ;

(চ) আইটি বিষয়ক শিক্ষা, গবেষণা ও উন্নয়নমূলক প্রতিষ্ঠান;

(ছ) নিরাপত্তা ও আইন শৃঙ্খলা রক্ষাকারী বাহিনী;

(জ) ডিজিটাল নিরাপত্তা সংশ্লিষ্ট বিশেষজ্ঞ ব্যক্তি, প্রতিষ্ঠান ও বিশ্ববিদ্যালয়;

(ঝ) আন্তর্জাতিক কম্পিউটার ইমার্জেন্সি রেসপন্স টিম ও বিশেষজ্ঞ ব্যক্তি বা প্রতিষ্ঠান;

(ঞ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তার সহিত সংশ্লিষ্ট ব্যক্তি বা প্রতিষ্ঠান;

(ট) টেলিযোগাযোগ সংশ্লিষ্ট সংস্থা বা প্রতিষ্ঠান।

১১। **ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনা সম্পর্কে ব্যবস্থা গ্রহণ**।—(১) জাতীয় কম্পিউটার এমার্জেন্সি রেসপন্স টিম উপবিধি (৩) এ বর্ণিত সকল ধরনের ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনা সম্পর্কে এবং দেশের অভ্যন্তরে সংঘটিত হইয়াছে বা সংঘটিত হইতে পারে এমন সকল ঘটনার বিষয়ে ব্যবস্থা গ্রহণ করিবে এবং উক্ত উদ্দেশ্যে জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম, এজেন্সি কর্তৃক নির্ধারিত সময়ে, উক্তরূপ ঘটনার মাত্রা অনুযায়ী উহা মোকাবেলা ও নিরসনের ব্যবস্থা গ্রহণ করিবে।

(২) কার্যসম্পাদন ও সেবা প্রদানের ক্ষেত্রে, জাতীয় কম্পিউটার এমার্জেন্সি রেসপন্স টিম নিম্নবর্ণিত ধরনের ডিজিটাল নিরাপত্তা সংক্রান্ত ঘটনাসমূহ বিবেচনা করিবে, যথাঃ—

(ক) গুরুত্বপূর্ণ নেটওয়ার্ক বা সিস্টেমের উদ্দেশ্যপূর্ণ অভিবীক্ষণ ;

(খ) গুরুত্বপূর্ণ সিস্টেম বা তথ্যের আপোষমূলক ব্যবস্থা গ্রহণ;

(গ) আইসিটি সিস্টেম বা তথ্য-উপাত্তে অননুমোদিত প্রবেশ;

(ঘ) ওয়েবসাইটের ক্ষতিসাধন বা অননুমোদিত প্রবেশ, পরিবর্তন সাধন (যথাঃ ক্ষতিকর প্রোগ্রাম প্রবেশ করানো বা কোনো ওয়েবসাইটের সহিত অন্য কোনো অনুমোদিত ওয়েবসাইটের সংযুক্ত (Link), ইত্যাদি);

(ঙ) ক্ষতিকর প্রোগ্রাম দ্বারা আক্রমন (যথাঃ ভাইরাস, ওয়ার্ম, ট্রোজান, বটনেটস, স্পাইওয়্যার);

(চ) সার্ভার আক্রমণ (যথাঃ ডাটাবেজ, মেইল, ডোমেইন নেম সিস্টেম (DNS), নেটওয়ার্ক ডিভাইস ইত্যাদি);

(ছ) ছদ্মবেশ গ্রহণক্রমে অনুপ্রবেশ (Phishing), স্পুফিং এবং পরিচয় প্রতারণা বা ছদ্মবেশ ধারণ;

(জ) সেবা প্রদানে অস্বীকার করা (Denial of Service), সেবা ও শ্রেণিকৃত সেবা প্রদানে অস্বীকার করা (Distributed Denial of Service);

(ঝ) গুরুত্বপূর্ণ তথ্য পরিকাঠামো, স্ক্যাডা সিস্টেম এবং ওয়্যারলেস নেটওয়ার্কের উপর হামলা;

(ঞ) ই-কর্মাস ও ই-গভর্নেন্স জাতীয় এপ্লিকেশনের উপর হামলা।

(৩) এই বিধির অধীন ব্যবস্থা গ্রহণের ক্ষেত্রে জাতীয় কম্পিউটার ইমার্জেন্সি রেসপন্স টিম নিম্নবর্ণিত বিষয়সমূহ, পর্যায়ক্রমে, বিবেচনা করিতে পারিবে, যথাঃ—

(ক) ব্যক্তি বা জনসাধারণের নিরাপত্তা ঝুঁকির আশঙ্কা;

(খ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর মূল নেটওয়ার্ক কাঠামো সংকটাপন্ন হওয়া;

(গ) আইডেন্টিটি চুরি, ডিজিটাল ডিভাইসে অবৈধ প্রবেশ এবং ওয়েবসাইট বিকৃতিকরণ;

(ঘ) ব্যক্তিগত একাউন্টের তথ্য চুরি;

(ঙ) দফা (ক) হইতে দফা (ঘ) এ উল্লিখিত ক্ষেত্র ব্যতীত অন্যান্য ক্ষেত্রে ডিজিটাল নিরাপদ সংক্রান্ত ঘটনার তীব্রতা ও ঝুঁকির ব্যাপকতা।

(৪) জাতীয় কম্পিউটার এমার্জেন্সি রেসপন্স টিম কর্তৃক উহার দায়িত্ব ও কার্যসম্পাদন সত্ত্বেও, ডিজিটাল তথ্য নিরাপত্তা ও ঝুঁকিমুক্ত রাখিবার দায়িত্ব সংশ্লিষ্ট ব্যক্তি বা প্রতিষ্ঠানের উপর ন্যস্ত থাকিবে।

(৫) এই বিধির অধীন ব্যবস্থা গ্রহণের ক্ষেত্রে, জাতীয় কম্পিউটার এমার্জেন্সি রেসপন্স টিম দেশ ও বিদেশের ডিজিটাল নিরাপত্তা বিষয়ে বিশেষায়িত প্রতিষ্ঠান, জাতীয় গোয়েন্দা ও আইন প্রয়োগকারী সংস্থা ও বিশেষায়িত ফরেনসিক ল্যাব, আইটি বিষয়ক শিক্ষা ও গবেষণা বিষয়ক প্রতিষ্ঠান বা ডিজিটাল নিরাপত্তা সংশ্লিষ্ট বিশেষজ্ঞ ব্যক্তি, বিশ্ববিদ্যালয় বা প্রতিষ্ঠানের সহযোগিতা গ্রহণ করিতে পারে।

১২। **গুরুত্বপূর্ণ তথ্য পরিকাঠামোর মূল্যায়ন**।—(১) নিম্নবর্ণিত ৪ (চার) পর্যায়ে এজেন্সি কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোর নিরাপত্তা মূল্যায়ন (evaluate) করিবে, যথাঃ—

(ক) পর্যায়-১ঃ এজেন্সি, নিম্নবর্ণিত বিষয়সমূহ বিবেচনা করিয়া, গুরুত্বপূর্ণ তথ্য পরিকাঠামোর কাজের সংকটপূর্ণ পরিধি (Critical Business Process), ডিজিটাল পরিসম্পদ, অন্তর্মুখী ও বহির্মুখী নির্ভরশীলতা, বিদ্যমান ডিজিটাল নিরাপত্তার নিয়ন্ত্রণসহ যাচাই করিবে, যথাঃ—

(অ) ডিজিটাল নিরাপত্তা কাঠামো;

(আ) তথ্য ব্যবস্থা;

(ই) শিল্প সংক্রান্ত নিয়ন্ত্রণ ব্যবস্থা (Industrial control system);

(ঈ) নেটওয়ার্ক;

(উ) সেবাসমূহ;

(ঊ) ত্রুটি-নির্দেশনা (Criticalities);

(ঋ) পরস্পর সংযুক্ততা বা পরনির্ভরশীলতা।

(খ) পর্যায়-২ঃ এজেন্সি, গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তার ভঙ্গুরতা, ঝুকি ও হুমকি মূল্যায়ন করিবে এবং এইক্ষেত্রে ধারাবাহিকভাবে প্রথম পর্যায়ের প্রযুক্তিগত ও পদ্ধতিগত নিরাপত্তা নিয়ন্ত্রণের বিষয়াদি চিহ্নিত করিবে;

(গ) পর্যায়-৩ঃ এজেন্সি, সমন্বিতরূপে, গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা নিয়ন্ত্রণ ব্যবস্থা এবং উক্ত পরিকাঠামোর কার্যক্রমের মূল্যায়ন করিবে;

(ঘ) পর্যায়-৪ঃ এজেন্সি প্রয়োগকৃত নিরাপত্তা নিয়ন্ত্রণ ব্যবস্থার বাস্তবায়ন করিবে এবং উক্ত উদ্দেশ্যে এজেন্সি উক্তরূপ নিয়ন্ত্রণ ব্যবস্থা তথ্যপ্রযুক্তির নিরীক্ষার ব্যবস্থা করিবে।

(২) এজেন্সি উপবিধি (১) এর অধীন গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা ব্যবস্থা মূল্যায়নের সময় অনুসরণীয় মূল্যায়ন কাঠামোসহ তথ্যপ্রযুক্তি নিরীক্ষা পদ্ধতি প্রণয়ন করিতে পারিবে।

১৩। **ডিজিটাল ফরেনসিক ল্যাব স্থাপন**।—(১) আইনের ধারা ১০ এর উপ-ধারা (১) এর উদ্দেশ্য পূরণকল্পে, এজেন্সি, জাতীয় ডিজিটাল নিরাপত্তা কাউন্সিলের নির্দেশনা ও পরামর্শ গ্রহণক্রমে, এক বা একাধিক ফরেনসিক ল্যাব স্থাপন করিবে।

(২) উপবিধি (১) এর অধীন স্থাপিত ডিজিটাল ফরেনসিক ল্যাব এজেন্সির অনুমোদন সাপেক্ষে পরিচালিত হইবে।

১৪। **ডিজিটাল ফরেনসিক ল্যাব কর্তৃক অনুসরণীয় মানদন্ড**।—(১) ডিজিটাল ফরেনসিক ল্যাব ডিজিটাল ফরেনসিক কার্যক্রমের মান নিশ্চিত করিবে এবং ব্যবহারিক দিক হইতে ডিজিটাল ফরেনসিক ল্যাব সাধারণত ISO/IEC/BDS 17025, ISO/IEC/BDS 15489, ISO/IEC/BDS 27037, ISO/IEC/BDS 27041, ISO/IEC/BDS 27042, ISO/IEC/BDS 27043, ISO/IEC/BDS 27050 কর্তৃক নির্ধারিত মানদন্ড অনুসরণ করিবে।

(২) উপবিধি (১) এর অধীন গুনগত মান নিশ্চিত করিবার ক্ষেত্রে, ডিজিটাল ফরেনসিক ল্যাব—

(ক) উপবিধি (১) এ উল্লিখিত মানদন্ড অনুসরণক্রমে এবং যথোপযুক্ত যোগ্যতাসম্পন্ন ও প্রশিক্ষণপ্রাপ্ত ব্যক্তি দ্বারা উহার অধীন সম্পাদিত ফরেনসিক বিশ্লেষণের জন্য এতদউদ্দেশ্যে প্রণীত গাইডলাইন অনুসরণক্রমে উহার কার্যক্রম পরিচালনা করিবে;

(খ) ডিজিটাল ফরেনসিক বিশ্লেষণের কার্যক্রমের গুনগত মান বজায় রাখিবে;

(গ) ডিজিটাল বিশ্লেষণের যথাযথ প্রক্রিয়া অনুসরণ করিবে;

(ঘ) ফরেনসিক বিশ্লেষণের কারিগরি মান বজায় রখিবার জন্য যথাযথ যন্ত্রপাতি ও সরঞ্জাম ব্যবহার করিবে;

(ঙ) উহার ভৌত অবকাঠামোগত সুযোগ সুবিধার ব্যবস্থা রাখিবে;

(চ) উহার অধীন সংরক্ষিত তথ্যাদির নিরাপত্তা ও গোপনীয়তা বজায় রাখিবে।

(৩) কার্যসম্পাদনের ক্ষেত্রে, ডিজিটাল ফরেনসিক ল্যাবকে—

(ক) নূতন প্রযুক্তিগত কার্যপদ্ধতি প্রয়োগের পূর্বে উহার পরীক্ষণ মাপকাঠির কার্যক্ষমতা সম্পর্কে নিশ্চিত হইতে হইবে;

(খ) ফরেনসিক নমুনার যথাযথ মান ব্যবহার করিতে হইবে;

(গ) পরীক্ষণের কাজে ব্যবহার্য যন্ত্রপাতি ও সরঞ্জামাদির যথাযথভাবে ক্রমাঙ্কিত (Calibrate) ও রক্ষণাবেক্ষণ করিতে হইবে;

(ঘ) ডিজিটাল ফরেনসিক ল্যাবে কর্মরত ব্যক্তিগণকে বিশেষজ্ঞ সাক্ষী হিসেবে সাক্ষ্য প্রদানে যোগ্যতা অর্জন করিতে হইবে এবং উক্ত উদ্দেশ্যে ফরেনসিক টুলস ও অন্যান্য বিষয়ে দক্ষতা অর্জনের জন্য যথাযথ প্রশিক্ষণ প্রদান করিতে হইবে এবং যন্ত্র ও সফটওয়্যার ব্যবহারের সনদ প্রদানের ব্যবস্থা রাখিতে হইবে।

১৫। **সাক্ষ্যের ফরেনসিক বিশ্লেষণ**।—(১) ডিজিটাল ফরেনসিক ল্যাবের ডিজিটাল ফরেনসিক বিশেষজ্ঞ ডিজিটাল সাক্ষ্যের ফরেনসিক বিশ্লেষণ করিবেন এবং উক্ত বিষয়ে তফসিল এ বর্ণিত পদ্ধতিতে বিশেষজ্ঞ মতামত প্রদান করিবেন।

(২) উপবিধি (১) এর অধীন প্রদত্ত বিশেষজ্ঞ মতামতে বিশ্লেষণ বা পরীক্ষাকার্য সম্পাদনকারী ব্যক্তির নাম ও স্বাক্ষর থাকিবে।

১৬। **ডিজিটাল ফরেনসিক ল্যাবের জনবল**।—(১) এজেন্সির অনুমোদিত সাংগঠনিক কাঠামো অনুযায়ী ডিজিটাল ফরেনসিক ল্যাবের প্রয়োজনীয় জনবল থাকিবে এবং উক্ত ল্যাবের কার্যাবলী সুষ্ঠুভাবে সম্পাদনের লক্ষ্যে এজেন্সি, প্রযোজ্য বিধি-বিধান অনুসরণক্রমে প্রয়োজনীয় সংখ্যক কর্মচারী নিয়োগ করিতে পারিবে।

(২) ডিজিটাল ফরেনসিক ল্যাবে অন্যূন ১(এক) জন করিয়া ডিজিটাল ফরেনসিক ল্যাব সুপারভাইজার ও ডিজিটাল ফরেনসিক ল্যাব বিশেষজ্ঞ থাকিবে।

(৩) ডিজিটাল ফরেনসিক ল্যাব সুপারভাইজার এর দায়িত্ব হইবে নিম্নরূপ, যথা:—

(ক) সিনিয়র ফরেনসিক বিশেষজ্ঞ হিসেবে দায়িত্ব পালন;

(খ) আইন ও এই বিধিমালায় বর্ণিত মানদন্ড নিয়ন্ত্রণের উদ্দেশ্যে নিয়োজিত ল্যাব কর্মকর্তাদের প্রশিক্ষণ নিশ্চিতকরণ;

(গ) ল্যাবে কর্মরত কর্মকর্তাগনের বাৎসরিক কর্মদক্ষতা মূল্যায়ণ;

(ঘ) ল্যাব কর্মকর্তাগণের প্রস্তুতকৃত প্রামাণিক দলিল বা প্রতিবেদনের প্রশাসনিক ও কারিগরি পর্যালোচনাকরণ;

(ঙ) ল্যাব কর্মকর্তাগণের পারদর্শিতা ও দক্ষতা যাচাইকরণ;

(চ) ল্যাবের হার্ডওয়্যার, সফটওয়্যার ও অন্যান্য যন্ত্রপাতির সঠিক কার্যকারিতা নিশ্চিতকরণ;

(ছ) ফরেনসিক কার্যে ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যারের গুনগতমান ও বৈধতা নিশ্চিতকরণ;

(জ) ফরেনসিক ল্যাবের উপযোগী হার্ডওয়্যার ও সফটওয়্যার ব্যবহারের সুপারিশকরণ।

(৪) ডিজিটাল ফরেনসিক ল্যাব বিশেষজ্ঞের দায়িত্ব হইবে নিম্নরূপ, যথা:—

(ক) ইলেক্ট্রনিক যন্ত্র হইতে তথ্য উপাত্ত সংগ্রহ ও পুনরুদ্ধার;

(খ) ডিজিটাল তথ্য সংগ্রহ ও পুনরুদ্ধারের ভিত্তিতে নিরপেক্ষ প্রতিবেদন প্রস্তুতকরণ;

(গ) মামলার কারিগরি ও প্রশাসনিক প্রতিবেদন পর্যালোচনা;

(ঘ) ফরেনসিক নমুনা বা ডিজিটাল আলামত চিহ্নিতকরণের নিমিত্ত অপরাধ সংঘটিত হইবার স্থানে আইন প্রয়োগকারী সংস্থাকে সহযোগিতা করা;

(ঙ) আদালতে তথ্য উপাত্তের সত্যতা যাচাইয়ে প্রামাণিক সাক্ষ্য প্রদান;

(চ) কর্মকর্তাগণকে হাতে-কলমে প্রশিক্ষণ, পরামর্শ ও দিক নির্দেশনা প্রদান;

(ছ) ফরেনসিক কার্যে ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যার গুণগতমান ও কার্যকারিতা নিশ্চিতকরণ;

(জ) ফরেনসিক মামলায় ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যার এর কর্মক্ষমতা নিশ্চিতকরণ।

১৭। **গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনাকারী ব্যক্তি বা প্রতিষ্ঠান কর্তৃক অনুসরণীয় বাধ্যবাধকতা**।—(১) গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনাকারী ব্যক্তি বা প্রতিষ্ঠান ডিজিটাল নিরাপত্তা নিশ্চিতকরণের লক্ষ্যে নিম্নবর্ণিত ব্যবস্থা গ্রহণ করিবে, যথাঃ—

(ক) অভ্যন্তরীন ডিজিটাল নিরাপত্তা ব্যবস্থাপনা ও পরিচালনা বিধি প্রস্তুতকরণ;

(খ) কম্পিউটার ভাইরাস, সাইবার আক্রমণ এবং অবৈধ অনুপ্রবেশ রোধে প্রযুক্তিগত নিরাপদ সুরক্ষা ব্যবস্থা গ্রহণ;

(গ) নেটওয়ার্ক কার্যক্রম পরিচালনা, পর্যবেক্ষণ ও উহার নিরাপত্তা লঙ্ঘনের ঘটনার রেকর্ডফাইল সংরক্ষণ;

(ঘ) সংরক্ষিত তথ্যের শ্রেণিকরণ;

(ঙ) ডিজিটাল নিরাপত্তা ব্যবস্থাপনা সম্পর্কে জ্ঞান রহিয়াছে এরূপ কর্মকর্তা নিয়োগ;

(চ) ডিজিটাল নিরাপত্তা কার্যে নিয়োজিত কর্মকর্তাদের ডিজিটাল নিরাপত্তা বিষয়ে শিক্ষা, প্রশিক্ষণ ও পরীক্ষণের ব্যবস্থা গ্রহণ;

(ছ) ডিজিটাল নিরাপত্তা লঙ্ঘনের ঘটনা ব্যবস্থাপনার অনুশীলন।

(২) গুরুত্বপূর্ণ তথ্য পরিকাঠামো শুধুমাত্র এজেন্সি কর্তৃক অনুমোদিত গুরুত্বপূর্ণ নেটওয়ার্ক পণ্য বা বিশেষায়িত নেটওয়ার্ক নিরাপত্তা পণ্য ক্রয় ও ব্যবহার করিতে পারিবে।

(৩) এজেন্সির পূর্ব অনুমোদন ব্যতিরেকে, গুরুত্বপূর্ণ তথ্য পরিকাঠামো জাতীয় নিরাপত্তা বিঘ্নিত হইতে পারে এরূপ কোনো পণ্য বা সেবা ক্রয় করিতে পারিবে না।

(৪) কোনো ব্যক্তির সংগৃহিত ও সঞ্চালিত ব্যক্তিগত ও গুরুত্বপূর্ণ তথ্য স্থানীয়ভাবে সংগ্রহ করিতে হইবে এবং এজেন্সির পূর্ব অনুমোদন ব্যতিরেকে, উক্তরূপ কোনো তথ্য দেশের বাহিরে স্থানান্তর করা যাইবে না।

(৫) গুরুত্বপূর্ণ তথ্য পরিকাঠামো পরিচালনাকারী প্রতিষ্ঠানসমূহ অনুমোদিত বা উপহার হিসেবে প্রদানকৃত কোনো সিস্টেম, সফটওয়্যার, বা অন্য কোনো নেটওয়্যার্ক পণ্য নিরাপত্তাজনিত পরীক্ষা ব্যতীত ব্যবহার করিতে পারিবে না।

১৮। **গুরুত্বপূর্ণ তথ্য পরিকাঠামো নিরীক্ষা**।—(১) প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো প্রতি ২ (দুই) বৎসর অন্তর বা কোনো বিশেষ পরিস্থিতিতে মহাপরিচালক কর্তৃক নির্দেশিত সময়ে এতদসংক্রান্ত অনুসরণীয় নীতিমালা ও কার্যসম্পাদনের মান যাচাই এর লক্ষ্যে, এজেন্সি কর্তৃক নির্ধারিত পদ্ধতিতে স্বীকৃত নিরীক্ষকের মাধ্যমে নিরীক্ষা কার্যসম্পাদনসহ প্রতি বৎসর ডিজিটাল নিরাপত্তা সংক্রান্ত ঝুঁকি নিরূপণ করিবে।

(২) উপবিধি (১) এর অধীন নিরীক্ষা কার্যক্রম ও ঝুঁকি নিরূপণ সম্পন্ন হইবার ৩০ (ত্রিশ) দিনের মধ্যে প্রত্যেক গুরুত্বপূর্ণ তথ্য পরিকাঠামো এতদ্‌সংক্রান্ত রিপোর্টের একটি কপি মহাপরিচালকের নিকট প্রেরণ করিবে।

(৩) যদি মহাপরিচালকের নিকট প্রতীয়মান হয় যে—

(ক) নিরীক্ষা কার্যক্রম যথাযথভাবে সম্পন্ন হয় নাই, তাহা হইলে তিনি উহা পুনরায় সম্পন্নের জন্য গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে নির্দেশ প্রদান করিতে পারিবেন;

(খ) নিরীক্ষা কার্যক্রম নির্দিষ্ট মান অনুযায়ী সন্তোষজনকভাবে সম্পাদিত হয় নাই এবং কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামো কর্তৃক বিভ্রান্তিকর ও অসম্পূর্ণ তথ্য প্রদান করা হইয়াছে, তাহা হইলে তিনি স্বীকৃত কোনো নিরীক্ষকের মাধ্যমে নিরীক্ষা কার্য সম্পাদনের জন্য নির্দেশ প্রদান করিতে পারিবেন;

(গ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তার ঝুঁকি নিরূপণ সংক্রান্ত কার্যক্রম সন্তোষজনকভাবে সম্পন্ন করা হয় নাই, তাহা হইলে তিনি গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে ডিজিটাল নিরাপত্তার হালনাগাদ অবস্থা মূল্যায়নের নিমিত্ত পুনরায় ব্যবস্থা গ্রহণের জন্য নির্দেশ প্রদান করিতে পারিবেন;

(ঘ) কোনো গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজাইন, আকার, নিরাপত্তা ও ক্রিয়া পদ্ধতি অননুমোদিতভাবে বস্তুগত পরিবর্তন আনয়ন করা হইয়াছে, তাহা হইলে তিনি উক্ত পরিকাঠামোকে পুনরায় নিরীক্ষা বা ডিজিটাল নিরাপত্তার ঝুঁকি নিরূপণক্রমে উহা সংশোধনের নির্দেশ প্রদান করিতে পারিবেন।

(৪) উপবিধি (৩) এর অধীন নিরীক্ষার যাবতীয় ব্যয় সংশ্লিষ্ট গুরুত্বপূর্ণ তথ্য পরিকাঠামোকে বহন করিতে হইবে।

১৯। **গুরুত্বপূর্ণ তথ্য পরিকাঠামো চিহ্নিতকরণ, ইত্যাদি**।—(১) আইনের ধারা ১৫ এর অধীন গুরুত্বপূর্ণ তথ্য পরিকাঠামো ঘোষণার ক্ষেত্রে নিম্নবর্ণিত বিষয়াদি বিবেচনা করিতে হইবে, যথা—

(ক) কোনো তথ্য-উপাত্ত বা কোনো ইলেক্ট্রনিক তথ্য নিয়ন্ত্রণ, প্রক্রিয়াকরণ, সঞ্চালন বা সংরক্ষণ করে এইরূপ কোনো তথ্য পরিকাঠামো ক্ষতিগ্রস্ত বা সংকটপূর্ণ হইলে উহা জননিরাপত্তা বা অর্থনীতি নিরাপত্তা বা জনস্বাস্থ্য বা জাতীয় নিরাপত্তা বা রাষ্ট্রীয় অখণ্ডতা বা সার্বভৌমত্বের উপর ক্ষতিকর প্রভাব সৃষ্টি করিবে কি না উহা নির্ধারণের ক্ষেত্রে ব্যবসা-বাণিজ্য, শিল্পকারখানা, ক্রেতা বা সরকারি পরিসেবার উপর কিরূপ প্রভাব পড়িবে উহা এবং উক্ত প্রতিষ্ঠানসমূহের দৈনিক আর্থিক লেনদেনের সমন্বিত মূল্য, প্রতিদিনের আর্থিক লেনদেনের সংখ্যা, সংযুক্ত সরঞ্জামাদির সংখ্যা ও উহার নেটওয়ার্কের আকার, উক্ত পরিকাঠামোর উপর অন্যান্য পরিকাঠামো নির্ভরতা ও অন্যান্য বিষয়াদির উপর সৃষ্ট প্রভাব;

(খ) জাতীয় নিরাপত্তা, অর্থনীতি, জনস্বাস্থ্য বা ব্যবসা-বাণিজ্য, শিল্পকারখানা, ক্রেতা বা সরকারি পরিসেবার উপর গুরুত্বপূর্ণ তথ্য পরিকাঠামো সংশ্লিষ্ট তথ্য ও যোগাযোগ প্রযুক্তির অবকাঠামোর অপ্রাপ্যতার প্রভাব, বিশেষ করিয়া স্বল্প সময়ে অপ্রাপ্যতার অধিকতর প্রভাবের মাত্রা নিরূপণ;

(গ) তথ্য ও যোগাযোগ প্রযুক্তির অবকাঠামো অচল বা বিনষ্ট হইবার ক্ষেত্রে উহার ভৌগোলিক ও পরিবেশগত প্রভাব,

(ঘ) গুরুত্বপূর্ণ তথ্য পরিকাঠামোর সেবা অপ্রাপ্যতার ক্ষেত্রে পূর্বোক্ত দফাসমূহে বর্ণিত প্রতিষ্ঠানসমূহের উপর সুদূরপ্রসারি প্রভাব।

২০। **সশ্লিষ্ট ব্যক্তি বা প্রতিষ্ঠানের সহায়তা গ্রহণ**।—আইন ও এই বিধিমালার বিধান কার্যকর করিবার ক্ষেত্রে কোনো বিশেষ পরিস্থিতির উদ্ভব হইলে উহা নিয়ন্ত্রণ বা উক্ত বিষয়ে কার্যসম্পাদনের জন্য মহাপরিচালক কর্তৃক নির্ধারিত সময়ে, ডিজিটাল নিরাপত্তার বিষয়ে অভিজ্ঞ ব্যক্তি, প্রতিষ্ঠান বা বিশেষজ্ঞের সহযোগিতা ও পরামর্শ গ্রহণ করা যাইবে এবং উক্তরূপে কোনো সহযোগিতা, পরামর্শ যাচনা করা হইলে সংশ্লিষ্ট ব্যক্তি, প্রতিষ্ঠান বা বিশেষজ্ঞ মহাপরিচালককে সহযোগিতা বা পরামর্শ প্রদান করিতে বাধ্য থাকিবে।

তফসিল

ডিজিটাল ফরেনসিক পরীক্ষা পদ্ধতিসমূহ

(বিধি ১৫ দ্রষ্টব্য)

প্রথম অধ্যায়

তথ্য প্রমাণ নির্ধারণ (Evidence Assessment)

তথ্য প্রমাণ নির্ধারণের ক্ষেত্রে নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা :—

(ক) **কার্যপ্রণালী**।—ডিজিটাল ফরেনসিক ল্যাবে প্রেরিত ফরেনসিক নমুনা বা মামলার আলামতসমূহ গ্রহণের সময় নিম্নবর্ণিত বিষয়াদি নিবিড়ভাবে পর্যবেক্ষণপূর্বক নিম্নবর্ণিত বিবরণ লিপিবদ্ধ করিতে হইবে, যথা :—

(অ) আলামত সংগ্রহের আইনগত ভিত্তি;

(আ) ফরেনসিক নমুনা বা আলামত সিলগালা করা রহিয়াছে কিনা; নিম্ন

(ই) ফরেনসিক নমুনা বা মামলার বর্ণনা;

(ঈ) সংশ্লিষ্ট হার্ডওয়্যার, সফটওয়্যার ও নথিসহ অন্যান্য প্রমাণাদি;

(উ) ফরেসনিক নমুনা বা আলামতের অবস্থা;

(ঊ) আলামত সংগ্রহের পারিপার্শ্বিক অবস্থা।

(খ) **ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা**।—(১) তদন্তকারী কর্মকর্তা নিম্নবর্ণিত বিষয়ে ফরেনসিক পরীক্ষার চাহিদা পর্যালোচনা করিবেন, যথা :—

(অ) ফরেনসিক পরীক্ষার চাহিদা প্রদানকারীর আইনগত ক্ষমতা;

(আ) ফরেনসিক পরীক্ষার চাহিদাপত্রের পরিপূর্ণতা নিশ্চিতকরণ;

(ই) চেইন অফ কাস্টডির পূর্ণাঙ্গ দলিল।

(২) তদন্তকারী কর্মকর্তার সহিত ফরেনসিক পরীক্ষার চাহিদা প্রদানকারীর আলোচনাপূর্বক তাহার চাহিদা এবং ফরেনসিক পরীক্ষার ফলাফলের সম্ভাব্যতার বিষয়ে অবহিত করাসহ উক্ত আলোচনায় নিম্নোক্ত বিষয়াদি বিবেচনা করিতে হইবে, যথা :—

(ক) প্রদত্ত ফরেনসিক নমুনা বা আলামতের ফরেনসিক পরীক্ষার জন্য অতিরিক্ত কোনো বিশেষায়িত পরীক্ষার প্রয়োজন রহিয়াছে কি না (যথা : Search key words, Tool marks, Trace and questioned documents ইত্যাদি);

(খ) সম্পূরক ফরেনসিক নমুনা বা ডিজিটাল আলামত সংগ্রহ (যথা : ইন্টারনেট সেবাদানকারীকে লগ সংরক্ষণ বা প্রদান এর আদেশ, দূরবর্তী তথ্য সংরক্ষণাগারের অবস্থান সনাক্তকরণ, ই-মেইল অধিগ্রহণ, ইত্যাদি);

(গ) তদন্তের স্বার্থে পারিপার্শ্বিক উপাদানের সম্পর্ক বিবেচনায় ফরেনসিক নমুনা বা ডিজিটাল আলামত ব্যতীত অন্যান্য নমুনা বা আলামত সংগ্রহ (যথা : জালিয়াতি বা প্রতারণার মামলার ক্ষেত্রে কম্পিউটার ব্যতিরেকে অন্যান্য উপাদান, যথা- ল্যামিনেটর, নিষ্ক্রিয় ক্রেডিট কার্ড, চেকবই, স্ক্যানার, প্রিন্টার ইত্যাদি);

(ঘ) সম্ভাব্য ফরেনসিক নমুনা বা ডিজিটাল আলামত চিহ্নিতকরণ (যথা : ছবি, স্প্রেডশীট, নথি, ডাটাবেস, আর্থিক রেকর্ড ইত্যাদি);

(ঙ) আক্রান্ত সিস্টেম হইতে অতিরিক্ত তথ্য অনুসন্ধানের প্রয়োজনীয়তা নির্ধারণ (যথা : ছদ্মনাম, ই-মেইল ঠিকানা, ব্যবহৃত ইন্টারনেট সেবাদানকারী প্রতিষ্ঠানের নাম, নেটওয়ার্ক কনফিগারেশন ও ব্যবহারকারী, সিস্টেম লগ, পাসওয়ার্ড, ব্যবহৃত নাম ইত্যাদি) এবং আক্রান্ত সিস্টেম সেবা প্রদানকারী প্রতিষ্ঠানের কর্মকর্তা ও উহার ব্যবহারকারীর নিকট হইতে অধিগ্রহণ;

(চ) আক্রান্ত কম্পিউটার ব্যবহারকারীদের দক্ষতা মুল্যায়ন;

(ছ) ফরেনসিক নমুনা বা ডিজিটাল আলামত বা প্রামাণিক তথ্য পরীক্ষার অগ্রাধিকার নির্ণয়;

(জ) ফরেনসিক পরীক্ষা পরিচালনার জন্য অতিরিক্ত জনবলের প্রয়োজনীয়তা নির্ধারণ;

(ঝ) ফরেনসিক পরীক্ষার জন্য প্রয়োজনীয় সরঞ্জাম নির্ধারণ।

দ্বিতীয় অধ্যায়

ফরেনসিক নমুনা বা আলামত অধিগ্রহণ (Acquisition)

ফরেনসিক নমুনা বা আলামত অধিগ্রহণের ক্ষেত্রে নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা :—

(ক) **কার্যপ্রণালী।**—নিম্নবর্ণিত বিষয়াদি বিবেচনা করিয়া ফরেনসিক পরীক্ষার জন্য ফরেনসিক নমুনা বা ডিজিটাল আলামত সংগ্রহ করিতে হইবে, যথা :—

(১) মূল ফরেনসিক নমুনা বা ডিজিটাল আলামতের সংরক্ষণ ও সুরক্ষার লক্ষ্যে বিট বাই বিট ইমেজিং এর মাধ্যমে ফরেনসিক পরীক্ষার জন্য কপি প্রস্তুতকরণ;

(২) নির্বাচিত বা ব্যবহৃত হার্ডওয়্যার ও সফটওয়্যারের কনফিগারেশন সিস্টেম নথিভুক্তকরণ;

(৩) নির্বাচিত বা ব্যবহৃত কম্পিউটার সিস্টেমের হার্ডওয়্যার এবং সফটওয়্যারের কার্যক্রম যাচাইকরণ;

(৪) ডিজিটাল ডিভাইসের কেসিং উন্মুক্ত করিয়া স্টোরেজ ডিভাইসে বাহির হইতে প্রবেশাধিকার নিশ্চিতকরণ;

(৫) নির্ধারিত ডিজিটাল ডিভাইসকে স্থির তড়িৎ (Static Electricity) ও চৌম্বক ক্ষেত্র (Magnetic Field) হইতে সুরক্ষা নিশ্চিতকরণ;

(৬) ডিজিটাল ডিভাইসের ভিতর বা বাহিরে রক্ষিত বা উভয় ধরনের স্টোরেজ ডিভাইস চিহ্নিতকরণ;

(৭) ডিজিটাল ডিভাইসের ইন্টারনাল স্টোরেজ ডিভাইস এবং হার্ডওয়্যারের কনফিগারেশন লিপিবদ্ধকরণ;

(৮) ড্রাইভ এর কনফিগারেশন (যথা : মডেল, আকার, জাম্পার সেটিংস, লোকেশন, ড্রাইভ ইন্টারফেস) লিপিবদ্ধকরণ;

(৯) নির্ধারিত ডিজিটাল ডিভাইসের অভ্যন্তরীণ কম্পোনেন্ট বা যন্ত্রাংশ পরীক্ষাকরণ (যথা : সাউন্ড কার্ড, ভিডিও কার্ড, নেটওয়ার্ক কার্ডসহ মিডিয়া অ্যাক্সেস কন্ট্রোল এড্রেস (ম্যাক), পারসনাল কম্পিউটার মেমোরি কার্ড, ইন্টারন্যাশনাল অ্যাসোসিয়েশন (পিসিএমসিআইএ) কার্ড ইত্যাদি);

(১০) নির্ধারিত ডিজিটাল ডিভাইসের ডাটা ধ্বংস, ক্ষতি বা পরিবর্তন রোধকল্পে স্টোরেজ ডিভাইস এর পাওয়ার সাপ্লাই, মাদারবোর্ড ও ডাটা কেবলের সংযোগ বিচ্ছিন্নকরণ;

(১১) সন্দেহজনক ডিজিটাল ডিভাইসের সিস্টেম হইতে কনফিগারেশনের তথ্য নিয়ন্ত্রিত বুটের মাধ্যমে অধিগ্রহণ;

(১২) সন্দেহজনক ডিজিটাল ডিভাইসের CMOS/BIOS তথ্য নিয়ন্ত্রিত বুটের মাধ্যমে অধিগ্রহণ;

(১৩) সন্দেহজনক ডিজিটাল ডিভাইসের বুট সিকোয়েন্স পরীক্ষাকরণ (যথা : ফ্লপি বা সিডি-রম ড্রাইভ হইতে সিস্টেম বুট করিতে বিআইওএস পরিবর্তন করা যাইতে পারে);

(খ) গৃহীত ডিজিটাল ডিভাইসের ফরেনসিক পরীক্ষার নিমিত্ত সিস্টেমের তারিখ ও সময় রেকর্ড ও সংরক্ষণের অনুসরনীয় পদ্ধতি :

(১) ফরেনসিক পরীক্ষার লক্ষে সন্দেহজনক ডিজিটাল ডিভাইসের কার্যকারিতা (functionality) এবং ফরেনসিক বুট ডিস্ক পরীক্ষার লক্ষ্যে ফরেনসিক বুট ডিস্ক হইতে দ্বিতীয়বার নিয়ন্ত্রিত বুট কার্যকর করিতে হইবে।

(২) হার্ডডিস্কের সকল সংযোগ বিচ্ছিন্নক্রমে ফ্লপি বা ইউএসবি পোর্ট বা সিডি-রম বা ডিভিডি-রম ড্রাইভের সংযোগ নিশ্চিত করিতে হইবে;

(৩) ফরেনসিক বুট ডিস্কটি ফ্লপি বা ইউএসবি পোর্ট অথবা সিডি-রম ড্রাইভে রাখিতে হইবে এবং কম্পিউটার বুট করিবার সময় নিশ্চিত করিতে হইবে যে কম্পিউটারটি ফরেনসিক বুট ডিস্ক হইতে বুট করিতে হইবে।

(৪) স্টোরেজ ডিভাইসগুলি পুনরায় সংযুক্ত করিয়া তৃতীয় নিয়ন্ত্রিত বুট ব্যবহারের মাধ্যমে CMOS বা BIOS ড্রাইভের কনফিগারেশন তথ্য সংগ্রহ করিতে হইবে;

(৫) ফরেনসিক পরীক্ষার লক্ষ্যে নির্ধারিত ডিজিটাল ডিভাইসের স্টোরেজ ব্যবহার করিয়া কম্পিউটারটিকে দুর্ঘটনাক্রমে বুট করা হইতে বিরত রাখিতে, বুট সিকোয়েন্স ফ্লপি বা ইউএসবি পোর্ট বা সিডি-রম ড্রাইভে ফরেনসিক বুট ডিস্ক নিশ্চিত করিয়া ডিজিটাল ডিভাইসটিকে বুট করিতে হইবে;

(৬) ড্রাইভ কনফিগারেশন তথ্যাবলীতে লজিক্যাল ব্লক এড্রেস (এল বি এ), লার্জ ডিস্ক, সিলিন্ডার, হেড, সেক্টর (সিএইচএস) বা অটো ডিটেক্ট অন্তর্ভুক্ত হইবে।

(গ) পাওয়ার সিস্টেম ডাউন।—(১) ফরেনসিক পরীক্ষার লক্ষ্যে নির্ধারিত ডিজিটাল ডিভাইসের স্টোরেজ ডিভাইসটি বাহির করিয়া পরীক্ষকের সিস্টেমে সংযোগের মাধ্যমে তথ্য অধিগ্রহণ করিতে হইবে। পরীক্ষকের সিস্টেমে জব্দকৃত ডিভাইসকে সংযুক্ত করিবার জন্য যথাযথ ব্যবস্থা গ্রহণ করিতে হইবে এবং ব্যতিক্রমী পরিস্থিতিতে জব্দকৃত ডিজিটাল ডিভাইস হইতে স্টোরেজ ডিভাইসগুলি পৃথক না করিবার সিদ্ধান্ত গ্রহণ করা যাইতে পারে তবে এইক্ষেত্রে নিম্নবর্ণিত বিষয়সমূহ বিবেচনা করিতে হইবে, যথা :—

(ক) RAID (Redundant Array of Independent Disk) এর ক্ষেত্রে পৃথকভাবে ডিস্কগুলি অধিগ্রহণ করিলে প্রত্যাশিত ফলাফল অনিশ্চিত হইতে পারে;

(খ) ল্যাপটপের ড্রাইভে প্রবেশ করা কঠিন হইতে পারে কারণ মূল সিস্টেম হইতে ড্রাইভকে বিচ্ছিন্ন করা হইলে ল্যাপটপটি অকেজো হইতে পারে;

(গ) হার্ডওয়্যার নির্ভরতা (লিগাসি সরঞ্জাম) যথা- পুরাতন ড্রাইভ নূতন সিস্টেমের অনুপযোগী হইতে পারে;

(২) যে ডিজিটাল ডিভাইস ব্যবহার করিয়া অপরাধ সংঘটিত হইয়াছে উহাতে ফরেনসিক ল্যাব পরীক্ষকের নিয়ন্ত্রণ বহির্ভূত থাকায় নেটওয়ার্ক ডিভাইস ব্যবহার করিয়া তথ্য অধিগ্রহণ করিতে হইবে;

(৩) জব্দকৃত স্টোরেজ ডিভাইস হইতে ফরেনসিক পরীক্ষার জন্য নির্ধারিত স্টোরেজ ডিভাইসে তথ্য স্থানান্তরের ক্ষেত্রে এ স্টোরেজটি সম্পূর্ণরূপে নিষ্কন্টক, ভাইরাস মুক্ত ও পরিচ্ছন্ন হইবে যাহাতে স্থানান্তরিত তথ্যসমূহ অবিকৃতভাবে রক্ষিত থাকে। এইক্ষেত্রে Independent Cyclic Redundancy Cheek (CRC), Hashing, ইত্যাদি প্রযুক্তি ব্যবহার করিবার ক্ষেত্রে নিম্নবর্ণিত ব্যবস্থা গ্রহণ করা যাইবে, যথা :—

(ক) নির্বাচিত অধিগ্রহণ পদ্ধতির উপর নির্ভর করিয়া যদি হার্ডওয়্যার রাইট প্রটেকশন ব্যবহার করা হইয়া থাকে, তাহা হইলে এই প্রক্রিয়াটি ইতোমধ্যে সম্পন্ন হইয়াছে বলিয়া গণ্য হইবে;

(খ) জব্দকৃত ডিভাইসটির রাইট প্রটেকশন ইনস্টল করিতে হইবে;

(গ) ফরেনসিক ল্যাবের নিজস্ব সিস্টেম হইতে বুট করিতে হইবে (ডিভাইসটি Non-Bootable অবস্থায় সংযুক্ত থাকিবে);

(ঘ) যদি সফ্টওয়্যার রাইট প্রটেকশন ব্যবহার করা হইয়া থাকে, তাহা হইলে ফরেনসিক ল্যাবের নিজস্ব সিস্টেম হইতে বুট করিতে হইবে এং সফটওয়্যার রাইট প্রটেকশন সক্রিয় করিতে হইবে;

(ঙ) উপযুক্ত সফটওয়্যার ব্যবহারক্রমে জব্দকৃত ডিভাইসের স্টোরেজের পূর্ণাঙ্গ ধারণক্ষমতা ও ব্যবহৃত অব্যবহৃত এলাকাসমূহ চিহ্নিত করিতে হইবে;

(চ) স্টোরেজ ডিভাইস হইতে ইলেক্ট্রনিক সিরিয়াল নাম্বার, সাক্ষ্যপ্রমাণ, Stand Alone Software, Forensic Software Analysis Suite, Dedicated Hardware Device, ইত্যাদির মাধ্যমে ফরেনসিক ল্যাবের স্টোরেজে অবিকল কপি সংরক্ষণ করিতে হইবে;

(ছ) মূল এবং অনুলিপির কপি Sector-by-Sector তুলনা করিয়া অধিগ্রহীত তথ্যের মৌলিকত্ব (Originality) নিশ্চিত করিতে হইবে।

তৃতীয় অধ্যায়

ফরেনসিক নমুনা বা আলামত পরীক্ষা (Examination)

যথাযথ ফরেনসিক পদ্ধতি ব্যবহারের মাধ্যমে ডিজিটাল সাক্ষ্যপ্রমাণ পরীক্ষা করিতে হইবে এবং প্রযোজ্য ক্ষেত্রে মূল ফরেনসিক নমুনা বা আলামতের উপর পরীক্ষা করা হইতে বিরত থাকিতে হইবে। ফরেনসিক নমুনা বা আলামত পরীক্ষার ক্ষেতে নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা :—

(১) **প্রস্তুতি**।—পৃথক মিডিয়া ব্যবহার করিয়া Directory/Directories প্রস্তুত করিয়া ডিজিটাল সাক্ষ্যপ্রমাণ পুনরুদ্ধার বা আহরণ করিতে হইবে।

(২) **তথ্য আহরণ।**—নিম্নবর্ণিত ২ (দুই)টি পৃথক ভৌত এবং লজিক্যাল আহরণ পদ্ধতিতে তথ্য আহরণ করা যাইবে। ফাইল সিস্টেম বিবেচনা না করিয়া সমগ্র ফিজিক্যাল ড্রাইভ হইতে ভৌত পদ্ধতিতে এবং লজিক্যাল আহরণ পদ্ধতিতে, অপারেটিং সিস্টেম, ফাইল সিস্টেম, অ্যাপ্লিকেশন শ্রেণিবদ্ধ করিয়া ফাইল ও ডাটা পুনরুদ্ধার করিতে হইবে, যথা :—

(ক) **ভৌত আহরণ (Physical Extraction) :** এই পদ্ধতিতে ড্রাইভে যেই প্রকারের ফাইল সিস্টেম বিন্যস্ত থাকুক না কেন, নিম্নবর্ণিতভাবে শুধুমাত্র ভৌত স্তর হইতে ডটিা আহরণ করিতে হইবে, যথা :—

(অ) মূলশব্দ (Keyword) খুঁজিয়া বাহির করা, ফাইল সনাক্তকরণ (File Carving), এবং ভৌত ড্রাইভ হইতে অব্যবহৃত স্থান (Un-Allocated Space), বিভাজন টেবিল (partition table) বাহির করিতে হইবে;

(আ) যেই সকল তথ্য বা উপাত্ত অপারেটিং সিস্টেম বা ফাইল সিস্টেমের অন্তর্গত নয় সেইগুলি মূলশব্দ (Keyword) দ্বারা খুঁজিয়া বাহির করিতে হইবে;

(ই) যেই সকল তথ্য বা উপাত্ত অপারেটিং সিস্টেম বা ফাইল সিস্টেমের অন্তর্গত নয় সেইগুলি পুনরুদ্ধার ফাইল সনাক্তকরণ দ্বারা খুঁজিয়া বাহির করিতে হইবে;

(ঈ) সমগ্র হার্ড-ড্রাইভের ভৌত আকার নির্ধারণক্রমে Partition Table পরীক্ষা করিয়া ফাইল সিস্টেমের বিন্যাস বাহির করিতে হইবে;

(খ) **লজিক্যাল আহরণ (Logical Extraction) :** ড্রাইভে ফাইল সিস্টেমের ভিত্তিতে এই পদ্ধতিতে ডাটা, (যথা : সক্রিয় ফাইলসমূহ, মুছিয়া ফেলা ফাইল, ফাইলের মধ্যবর্তী স্থান, অবণ্টনকৃত স্থান ইত্যাদি) আহরণ করা হইয়া থাকে। ফাইল সিস্টেমের তথ্য আহরণ করিতে ফাইলের বিভিন্ন বৈশিষ্ট্য, যথা : ফাইলের অবকাঠামো, ফাইলের ধরণ, ফাইলের নাম, সাইজ, অবস্থান, তারিখ, সময় ও অন্যান্য বিষয়ের উপর নির্ভর করিয়া নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা :—

(অ) নির্ণীত হ্যাশ মানের সহিত বিশুদ্ধ ফাইলের হ্যাশ মানের তুলনা করিয়া পরিচিত ফাইল নিরূপন ও নির্ধারণ করিতে হইবে;

(আ) ড্রাইভে ফাইলের নাম ও ধরন, ফাইলের হেডার এবং অবস্থানের ভিত্তিতে পরীক্ষার জন্য প্রাসঙ্গিক ফাইলসমূহ আহরণ করিতে হইবে;

(ই) মুছিয়া ফেলা ফাইলসমূহ পুনরুদ্ধার করিতে হইবে;

(ঈ) পাসওয়ার্ড দ্বারা সুরক্ষিত, এনক্রিপ্টেড ও সঙ্কুচিত ফাইলসমূহ পুনরুদ্ধার করিতে হইবে;

(উ) ফাইলসমূহের মধ্যবর্তী ফাঁকা স্থান সনাক্তকরণ;

(ঊ) অবণ্টনকৃত স্থান সনাক্তকরণ।

(৩) **আহরিত ফাইলের বিশ্লেষণ।**—ঘটনার সময় আহরিত ডাটা কতটুকু গুরুত্বপূর্ণ উহা বিশ্লেষণপূর্বক ডাটা প্রক্রিয়াকরণের ক্ষেত্রে সময়সীমা, লুক্কায়িত ডাটা, অ্যাপ্লিকেশন ও ফাইল, সত্ত্বাধিকারী ও এখতিয়ার ইত্যাদি বিষয় বিশ্লেষণ করিবার সময় এইক্ষেত্রে কম্পিউটারের BIOS এ প্রদর্শিত সময়ের সহিত সিস্টেমে প্রদর্শিত সময়ের পার্থক্য নিম্নবর্ণিতরূপে বিবেচনা করিতে হইবে, যথা :—

(ক) **ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময়ের পর্যালোচনা ও বিশ্লেষণ (Timeframe Analysis) :** ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময় পর্যালোচনার মাধ্যমে ঘটনার সময়ের সহিত ব্যবহারকারীদের সংশ্লিষ্টতা সনাক্ত করা যায়। নিম্নবর্ণিত ২ (দুই) পদ্ধতিতে ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময় পর্যালোচনা ও বিশ্লেষণ করা যাইবে, যথা:—

(অ) সময়ের সহিত সম্পর্কিত ফাইল সিস্টেমের উপাত্ত (যথা: সর্বশেষ ফাইল সিস্টেমের Read বা Write বা Execute বা Protect অনুমতি পরিবর্তন, সর্বশেষ ব্যবহার, ফাইল সৃষ্টিকরণ এবং ফাইলের সর্বশেষ পরিবর্তন ইত্যাদি) তদন্তের মাধ্যমে নির্ধারিত ফাইলের সাথে ব্যবহারকারীদের সংশ্লিষ্টতা নির্ণয় করা যাইবে;

(আ) Error log, Application Installation Log, Connection Log, Security Log, ইত্যাদি বিষয় বিবেচনাক্রমে অ্যাপ্লিকেশন ও সিস্টেমের লগসমূহ বিশ্লেষণ করিতে হইবে।

(খ) **লুক্কায়িত ডাটার বিশ্লেষণঃ (Hidden Data Analysis):**—লুক্কায়িত ডাটার বিশ্লেষণের মাধ্যমে কম্পিউটারে গোপনীয় ডাটা সনাক্ত ও পুনরুদ্ধার করিবার ক্ষেত্রে নিম্নবর্ণিত পদ্ধতি অনুসরণ করিতে হইবে, যথা:—

(অ) ব্যবহারকারী ইচ্ছাকৃতভাবে বা উদ্দেশ্যমূলকভাবে তথ্য পরিবর্তন করিলে ফাইল হেডারকে ঐ ফাইলের এক্সটেনশন এর সহিত তুলনা (Correlate) করিয়া অসামঞ্জস্যতা চিহ্নিত করিতে হইবে;

(আ) সকল পাসওয়ার্ড দ্বারা সুরক্ষিত, এনক্রিপ্টেড ও সংকুচিত ফাইলে প্রবেশাধিকার স্থাপনপূর্বক অযাচিত বা অননুমোদিত হস্তক্ষেপ (Unauthorized Access) নির্ণয় করিতে হইবে;

(ই) Host Protected Area (HPA) এ প্রবেশ করিয়া উক্ত HPA এ ব্যবহারকারী কর্তৃক প্রস্তুতকৃত ডাটার উপস্থিতির ডাটা গোপন করিবার বিষয়টি চিহ্নিত করা যাইবে।

(গ) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis):** ডিজিটাল ডিভাইসের প্রোগ্রাম ও ফাইলসমূহে তদন্তের সহিত প্রাসঙ্গিক তথ্যসহ সিস্টেম ও ইহার ব্যবহারকারীর সক্ষমতা সম্পর্কে ধারণা লাভের নিমিত্ত নিম্নবর্ণিত পদ্ধতিতে বিবেচনা করিতে হইবে, যথা:—

(অ) প্রাসঙ্গিকতা ও প্যাটার্ন বিশ্লেষণের জন্য ফাইলসমূহের নাম পুনর্বিবেচনা;

(আ) ফাইলের বিষয়বস্তু পরীক্ষা;

(ই) ডিজিটাল ডিভাইসের অপারেটিং সিস্টেমসমূহের সংখ্যা ও ধরণ চিহ্নিতকরণ;

(ঈ) ডিজিটাল ডিভাইসে বিদ্যমান অ্যাপ্লিকেশনসমূহর সহিত সম্পর্কিত ফাইলের সামঞ্জস্যতা চিহ্নিতকরণ;

(উ) ডিজিটাল ডিভাইসের ফাইলসমূহের মধ্যে সামঞ্জস্যতা চিহ্নিতকরণ (যথা- ব্যবহারকারীর জব্দকৃত ডিজিটাল ডিভাইসের ইন্টারনেট হিস্টোরি লগের সহিত ব্রাউজারের ক্যাশ (Cache) ফাইল, ইমেইলের সহিত প্রেরিত সংযুক্তির (Attachment) ও সংশ্লিষ্ট ইমেইলের সামঞ্জস্যতা চিহ্নিতকরণ ইত্যাদি);

(ঊ) ডিজিটাল ডিভাইসের মধ্যকার অপরিচিত ফাইলের ধরণ এবং তদন্তের সহিত উহার সংশ্লিষ্টতা নির্ধারণ;

(ঋ) নির্ধারিত স্থান বা অন্য কোনো স্থানে রক্ষিত ডিজিটাল ডিভাইসের অ্যাপ্লিকেশন ও ইহার সংশ্লিষ্ট ফাইলের সংরক্ষণের স্থান নির্ণয়ের জন্য ব্যবহারকারীর সংরক্ষিত স্থান (Default Storage location) পরীক্ষা;

(এ) ডিজিটাল ডিভাইসের ব্যবহারকারীর কনফিগারেশন পরীক্ষা;

(ঐ) ডিজিটাল ডিভাইসের ফাইলের মেটাডাটা (ফাইল সম্পর্কিত তথ্য) বিশ্লেষণ করিয়া উহার বিষয়বস্তু পর্যালোচনাক্রমে মেটাডাটায় ফাইলের প্রণেতা (Author) কর্তৃক সর্বশেষ সংশোধনের (Edit) সময় কতবার উহা সংশোধন করা হইয়াছে, সেই তথ্য এবং ফাইল সম্পর্কিত অন্যান্য তথ্য অন্তর্ভূক্ত থাকিবে।

(ঘ) **মালিকানা ও ব্যবহারঃ** যেই ক্ষেত্রে, ডিজিটাল ডিভাইসের ফাইলের প্রণেতা, সংশোধনকারী, প্রবেশকারী, ডাটার মালিক ও জ্ঞাত ব্যবহারকারী নিরূপণ করিবার প্রয়োজনীয়তা উদ্ভূত হইলে সেই ক্ষেত্রে বিশ্লেষণের প্রয়োজনে নিম্নবর্ণিত বৈশিষ্ট্যসমূহ বিবেচনা করা যাইবে, যথা:—

(অ) **ডিজিটাল ডিভাইসের ব্যবহার সম্পর্কিত সময়ের পর্যালোচনা ও বিশ্লেষণ (Timeframe Analysis) :** ডিজিটাল ডিভাইসের ফাইলকে সুনির্দিষ্ট তারিখ ও সময়ের গন্ডিতে আবদ্ধ করিবার মাধ্যমে ইহার মালিক ও ব্যবহারকারী চিহ্নিতকরণ;

(আ) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis):** ডিজিটাল ডিভাইসের ফাইল অনির্ধারিত (Non-Default) স্থানে সংরক্ষণ (যথা: "শিশু পর্ণ (Child Porn)" নামে ডিজিটাল ডিভাইসের ব্যবহারকারী কর্তৃক একটি Directory প্রস্তুত করা;

(ই) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis):** ডিজিটাল ডিভাইসের ফাইলের নাম হইতে ফাইলের বিষয়বস্তু ও উহার সাক্ষ্যগত মূল্য সম্পর্কে ধারণা প্রাপ্তি;

(ঈ) **লুক্কায়িত ডাটার বিশ্লেষণঃ (Hidden Data Analysis):** সনাক্তকরণ এড়াইবার লক্ষ্যে ইচ্ছাকৃতভাবে ডাটা লুকাইয়া রাখা;

(ড) **লুক্কায়িত ডাটার বিশ্লেষণ (Hidden Data Analysis):** যেই ক্ষেত্রে পাসওয়ার্ড দ্বারা সুরক্ষিত ও এনক্রিপ্টেড (Encrypted) ফাইলের পুনরুদ্ধার করিতে হয়, সেই ক্ষেত্রে পাসওয়ার্ডের তত্ত্বাবধায়ককে মালিক বা ব্যবহারকারী হিসাবে চিহ্নিত করা যাইতে পারে;

(ঢ) **অ্যাপ্লিকেশন ও ফাইলের বিশ্লেষণ (Application and File Analysis):** ডিজিটাল ডিভাইসের ফাইলের বিষয়বস্তু হইতে ইহার মালিক বা ব্যবহারকারী চিহ্নিত করা যাইতে পারে।

(৪) **ফলাফল প্রাপ্তি:** প্রাপ্ত ফলাফল বিবেচনাক্রমে পূর্ণাঙ্গ প্রতিবেদন প্রস্তুত করিতে হইবে।

চতুর্থ অধ্যায়

নথিভূক্তকরণ ও প্রতিবেদন প্রস্তুতকরণ (Documentation & Reporting)

নথি ও প্রতিবেদন প্রস্তুতকরণের ক্ষেত্রে নিম্নবর্ণিত ধাপসমূহ অনুসরণ করিতে হইবে, যথা :—

(ক) কার্যপ্রণালী।—প্রতিবেদন স্বয়ংসম্পূর্ণ ও নির্ভুল হইতে হইবে এবং সংশ্লিষ্ট কর্তৃপক্ষের বোধগম্য করিয়া প্রণয়ন এবং বিদ্যমান নীতিমালা ও প্রযুক্তি অনুসরণপূর্বক প্রতিবেদন প্রস্তুত এবং সংরক্ষণ করিতে হইবে। পরীক্ষকের প্রতিবেদন প্রস্তুত করিবার সময় নিম্নবর্ণিত বিষয় অন্তর্ভুক্ত থাকিতে হইবে, যথা:—

(অ) তদন্তকারী কর্মকর্তা এবং ক্ষেত্রমত সংশ্লিষ্ট আইনজীবীর সহিত পরামর্শ করিবার সময় নোট গ্রহণ;

(আ) ডিজিটাল নমুনা বা আলামত সংগ্রহ পদ্ধতির অনুলিপি সংরক্ষণ;

(ই) ফরেনসিক পরীক্ষার চাহিদাপত্রের অনুলিপি সংরক্ষণ;

(ঈ) চেইন অব কাস্টডি এর অনুলিপি সংরক্ষণ;

(উ) কার্যক্রমের বিস্তারিত বিবরণ নথিতে লিপিবদ্ধকরণ;

(ঊ) নোট গ্রহণের তারিখ, সময়, বিবরণ এবং গৃহীত পদক্ষেপের ফলাফলসমূহ লিপিবদ্ধকরণ;

(ঋ) ফরেনসিক পরীক্ষার সময় পরিলক্ষিত অনিয়ম এবং গৃহীত পদক্ষেপ লিপিবদ্ধকরণ;

(এ) অতিরিক্ত তথ্যাদি (যথা: নেটওয়ার্ক টপোলজি (Topology), অনুমোদিত ব্যবহারকারীদের তালিকা, ব্যবহারকারীর চুক্তি (Agreement) এবং পাসওয়ার্ড (Password) অন্তর্ভুক্তকরণ);

(ঐ) সরকার বা সরকারি সংস্থা বা পরীক্ষকের নির্দেশে সিস্টেম বা নেটওয়ার্ক এ পরিবর্তন করিয়া থাকিলে উহা লিপিবদ্ধকরণ;

(ও) অপারেটিং সিস্টেম এবং সংশ্লিষ্ট সফ্টওয়্যারের বর্তমান সংস্করণ ও ইনস্টলকৃত পরিবর্তনসমূহ (Installed Patch) লিপিবদ্ধকরণ;

(ঔ) দূরবর্তী স্টোরেজ (Remote storage), প্রান্তিক ব্যবহারকারীর প্রবেশাধিকার (Remote user access) এবং অফসাইট ব্যাকআপ (offsite backups) সম্পর্কিত প্রাপ্ত তথ্য লিপিবদ্ধকরণ।

তবে যেইক্ষেত্রে পরীক্ষা চলাকালীন এইরূপ কিছু ফরেনসিক নমুনা বা ডিজিটাল আলামত পাওয়া যায় যাহার ফরেনসিক বিশ্লেষণ বর্তমানে প্রচলিত আইনী কাঠামোর আওতাধীন নহে, তাহা হইলে উক্ত বিষয়ে অতিরিক্ত অনুসন্ধানের জন্য বিষয়টি ডিজিটাল নিরাপত্তা এজেন্সির মহাপরিচালকের গোচরীভূত করিতে হইবে।

(খ) পরীক্ষকের প্রতিবেদন।—প্রতিবেদন প্রস্তুত করিবার সময় নিম্নলিখিত বিষয়সমূহ অন্তর্ভুক্ত করিতে হইবে, যথা:—

(১) প্রতিবেদক এজেন্সির পরিচয়;

(২) তদন্ত সনাক্তকারী বা জমা নম্বর;

(৩) তদন্তকারী কর্মকর্তার পরিচয়;

(৪) জমাদানকারীর পরিচয়;

(৫) প্রাপ্তির তারিখ;

(৬) প্রতিবেদনের তারিখ;

(৭) পরীক্ষার জন্য প্রাপ্ত ফরেনসিক নমুনা বা মামলার আলামতসমূহের সিরিয়াল নম্বর, প্রস্তুতকারক এবং মডেলসহ বিস্তারিত তালিকা;

(৮) পরীক্ষকের পরিচয় এবং স্বাক্ষর;

(৯) পরীক্ষার সময় গৃহীত পদক্ষেপসমূহের সংক্ষিপ্ত বিবরণ (যথা: স্ট্রিং অনুসন্ধান, গ্রাফিক্স চিত্র অনুসন্ধান এবং মুছিয়া ফেলা ফাইলসমূহ পুনরুদ্ধার ইত্যাদি);

(১০) ফলাফল ও উপসংহার।

(গ) **প্রাপ্ত ফলাফলের সার-সংক্ষেপ।**—প্রাপ্ত ডিজিটাল আলামতের ফরেনসিক পরীক্ষার সংক্ষিপ্ত ফলাফল প্রতিবেদনে লিপিবদ্ধ করিতে হইবে।

(ঘ) প্রাপ্ত ফলাফলের বিস্তারিত বিবরণ।—প্রত্যেক প্রতিবেদনে ফরেনসিক নমুনা বা ডিজিটাল আলামতের ফরেনসিক পরীক্ষার ফলাফলে নিম্নবর্ণিত বিষয়সমূহের বিস্তারিত বিবরণ লিপিবদ্ধ করিতে হইবে, যথা :

(১) চাহিদাপত্রের সহিত সম্পর্কিত জব্দকৃত ডিজিটাল ডিভাইসের ফাইলসমূহ;

(২) ফলাফলকে সমর্থন করিতে পারে এইরূপ মুছিয়া ফেলা ফাইলসহ অন্যান্য ফাইলসমূহ;

(৩) স্ট্রিং অনুসন্ধান, মূলশব্দ (Keyword) অনুসন্ধান এবং টেক্সট স্ট্রিং অনুসন্ধানের ফলাফল;

(৪) ইন্টারনেট সম্পর্কিত প্রমাণাদি বিশ্লেষণ (যথাঃ Web site traffic analysis, chat logs, cache files, e-mail, and news group activity);

(৫) গ্রাফিক চিত্র বিশ্লেষণ;

(৬) মালিকানা নির্ধারণ ও প্রোগ্রাম রেজিস্ট্রির তথ্যাদি;

(৭) প্রাসঙ্গিক তথ্য বিশ্লেষণ;

(৮) পরীক্ষিত ফরেনসিক নমুনা বা ডিজিটাল আলামতসমূহে বিদ্যমান প্রোগ্রামের বিবরণ;

(৯) তথ্য লুকাইয়া রাখা বা মাস্কিং করিবার জন্য ব্যবহৃত কৌশল, (যথাঃ এনক্রিপশন, স্টেগানোগ্রাফি) লুক্কায়িত তথ্যের বৈশিষ্ট্য, লুক্কায়িত পার্টিশন এবং অসংগতিপূর্ণ ফাইলসমূহের নাম।

রাষ্ট্রপতির আদেশক্রমে
এন এম জিয়াউল আলম পিএএ
সিনিয়র সচিব।

মোঃ তারিকুল ইসলাম খান, উপপরিচালক, বাংলাদেশ সরকারী মুদ্রণালয়, তেজগাঁও, ঢাকা কর্তৃক মুদ্রিত।
মোঃ আসাদুজ্জামান, উপপরিচালক (অতিঃ দায়িত্ব), বাংলাদেশ ফরম ও প্রকাশনা অফিস, তেজগাঁও, ঢাকা কর্তৃক প্রকাশিত। website : www.bgpress.gov.bd