# ভূমিসেবায় সাইবার নিরাপত্তা ও তথ্য সুরক্ষা নির্দেশিকা




ভূমি মন্ত্রণালয়
গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

**সংস্করণ ১.০, ২০২৬**



**৩০ জুন, ২০২৬**

## সূচিপত্র


১. ভূমিকা ..... ৯

১.১ শিরোনাম, প্রয়োগ ও প্রবর্তন: ..... ৯

১.২ সংজ্ঞা: ..... ৯

১.৩ লক্ষ্য ..... ১০

১.৪ পরিধি (Scope) ..... ১০

১.৫ প্রযোজ্যতা (Applicability) ..... ১১

১.৬. আইনগত ভিত্তি ..... ১১

১.৭ রেফারেন্স ও মানদণ্ড (References and Standards) ..... ১২

২. শাসন ও নিরাপত্তা ব্যবস্থাপনা (Governance and Security Management) ..... ১৩

২.১ তথ্য নিরাপত্তা নীতি (Information Security Policy) ..... ১৩

*২.১.১ স্ট্যান্ডার্ড অপারেটিং প্রসিডিউর (Standard Operating Procedures)* ..... ১৩

২.২ ভূমিকা ও দায়িত্ব (Roles and Responsibilities) ..... ১৫

*ক) সিনিয়র ম্যানেজমেন্ট (Senior Management)* ..... ১৬

*খ) CISO/ISO (Chief Information Security Officer/Information Security Officer):* ..... ১৬

*গ) ব্যক্তিগত উপাত্ত সুরক্ষা দায়িত্বপ্রাপ্ত কর্মকর্তা (Data Protection/Privacy Officer)* .... ১৭

*ঘ) আইটি অপারেশনস ও সিকিউরিটি টিম (IT Operations and Security Team)* ..... ১৮

*ঙ) সিস্টেমের মালিক ও তথ্য সম্পদের সংরক্ষক (System Owner and Information Asset Custodian)* ..... ১৮

*চ) সিস্টেম/অ্যাপ্লিকেশন ডেভেলপার, পরামর্শক, ভেন্ডর ও ঠিকাদার প্রতিষ্ঠান:* ..... ১৯

*ছ) সকল কর্মকর্তা/কর্মচারী প্রতিষ্ঠান:* ..... ১৯

২.৩ নিরাপত্তা শাসন কাঠামো (Security Governance Framework) ..... ২০

*২.৩.১. শাসন কাঠামো (Governance Structure)* ..... ২০

*২.৩.২. শাসন নীতি (Governance Principles)* ..... ২১

*২.৩.৩. নিরাপত্তা ব্যবস্থাপনা কার্যক্রম (Security Management Activities)* ..... ২১

২.৪ আইনগত ও কমপ্লায়েন্স চাহিদা (Compliance and Legal Requirements) ..... ২২

৩. সম্পদ ব্যবস্থাপনা (Asset Management) ..... ২৩

৩.১ তথ্য সম্পদের শ্রেণিবিন্যাস (Information Asset Classification) ..... ২৩

*৩.১.১ শ্রেণিবিন্যাস স্তরসমূহ:* ..... ২৩

*৩.১.২ ব্যক্তিগত উপাত্ত (Private/Personal Data):* ..... ২৩
৩.২ সম্পদ তালিকা ও মালিকানা (Asset Inventory and Ownership)..... ২৪
*৩.২.১ কেন্দ্রীয় সম্পদ তালিকা (Asset Register) যাতে অন্তর্ভুক্ত থাকবে-* ..... *২৪*
*৩.২.২ প্রত্যেক সম্পদের নির্ধারিত মালিক/কাস্টডিয়ান (Ownership) থাকবে, যাঁরা নিশ্চিত করবেন-২৪*
৩.৩ ডেটা হ্যান্ডলিং ও লেবেলিং (Data Handling and Labelling)..... ২৫
*৩.৩.১ সংবেদনশীল ডেটা যথাযথভাবে সুরক্ষিত রাখতে শ্রেণিবিন্যাস অনুযায়ী লেবেলিং ও হ্যান্ডলিং করতে হবে।* ..... *২৫*
*৩.৩.২ অপসারণযোগ্য মিডিয়া ব্যবস্থাপনা (Removable Media Management)*..... *২৫*
৩.৪ সম্পদের গ্রহণযোগ্য ব্যবহার (Acceptable Use of Assets) ..... ২৬
৩.৫ সম্পদের জীবনচক্র ব্যবস্থাপনা (Asset Lifecycle Management)..... ২৬
**৪. তথ্য নিরাপত্তা ঝুঁকি ব্যবস্থাপনা (Information Security Risk Management) ..... ২৮**
৪.১ ঝুঁকি ব্যবস্থাপনা কাঠামো (Risk Management Framework - RMF) ..... ২৮
*৪.১.১ ঝুঁকি মূল্যায়নের মানদণ্ড (Risk Criteria)*..... *২৮*
৪.২ ঝুঁকি মূল্যায়ন ও মোকাবিলা (Risk Assessment and Treatment)..... ২৯
৪.৩ ঝুঁকি নিবন্ধন ও ট্র্যাকিং (Risk Register and Mitigation Tracking) ..... ২৯
৪.৪ তৃতীয় পক্ষের ঝুঁকি ব্যবস্থাপনা (Third-Party Risk Management)..... ৩০
**৫. সরবরাহকারী নিরাপত্তা ব্যবস্থাপনা (Supplier Security Management) ..... ৩২**
৫.১ সরবরাহকারী মূল্যায়ন ও যথাযথ সতর্কতা (Supplier Evaluation and Due Diligence)..... ৩২
৫.২ চুক্তিভিত্তিক নিরাপত্তা শর্ত (Contractual Security Requirements)..... ৩২
৫.৩ তৃতীয় পক্ষের প্রবেশাধিকার নিয়ন্ত্রণ (Third-Party Access Controls) ..... ৩২
৫.৪ সরবরাহকারী ঝুঁকি মূল্যায়ন (Supplier Risk Assessment)..... ৩৩
৫.৫ সরবরাহকারীর কার্যকারিতা পর্যবেক্ষণ ও পর্যালোচনা (Monitoring and Review of Supplier Performance)..... ৩৩
**৬. নিরাপত্তা ব্যবস্থাপনা ও প্রক্রিয়া (Security Management and Procedures) ..... ৩৪**
৬.১ গ্রহণযোগ্য ব্যবহার নীতি (Acceptable Use Policy)..... ৩৪
৬.২ পাসওয়ার্ড ব্যবস্থাপনা (Password Management) ..... ৩৪
৬.৩ রিমোট এক্সেস ব্যবস্থাপনা (Remote Access Management)..... ৩৫
৬.৪ এনক্রিপশন ব্যবস্থাপনা (Encryption Management) ..... ৩৫

৬.৫ কর্মীদের দায়িত্ব ও আচরণবিধি (Employee Responsibilities and Code of Conduct) ..... ৩৫
৭. প্রবেশাধিকার নিয়ন্ত্রণ (Access Control) ..... ৩৭
৭.১ ব্যবহারকারীর প্রবেশাধিকার জীবনচক্র ব্যবস্থাপনা (User Access Lifecycle Management) ..... ৩৭
৭.১.১ *Onboarding (নতুন ইউজার):* ..... ৩৭
৭.১.২ *Modification (পরিবর্তন):* ..... ৩৭
৭.১.৩ *Offboarding (ইউজার নিষ্ক্রিয়করণ):* ..... ৩৭
৭.২ ভূমিকা-ভিত্তিক প্রবেশাধিকার নিয়ন্ত্রণ (Role-Based Access Control - RBAC) ..... ৩৭
৭.৩ প্রিভিলেজড অ্যাক্সেস ম্যানেজমেন্ট (Privileged Access Management - PAM) ... ৩৮
৭.৪ প্রবেশাধিকার রিভিউ ও ডিপ্রভিশনিং (Access Review and De-Provisioning) ..... ৩৮
৭.৫ লজিক্যাল অ্যাক্সেস কন্ট্রোল (Applications, OS, DB, Network, Endpoints) ..... ৩৯
১. *Applications:* ..... ৩৯
২. *Operating Systems (OS):* ..... ৩৯
৩. *Databases:* ..... ৩৯
৪. *Networks:* ..... ৩৯
৫. *Endpoints:* ..... ৩৯
৮. সিস্টেম ও নেটওয়ার্ক নিরাপত্তা (System and Network Security) ..... ৪০
৮.১ সিস্টেম হার্ডেনিং ও কনফিগারেশন ব্যবস্থাপনা (System Hardening and Configuration Management) ..... ৪০
৮.২ প্যাচ ও দুর্বলতা ব্যবস্থাপনা (Patch and Vulnerability Management) ..... ৪০
৮.৩ নেটওয়ার্ক নিরাপত্তা স্থাপত্য (Network Security Architecture) ..... ৪১
৮.৪ ফায়ারওয়াল ও পেরিমিটার কন্ট্রোলস (Firewall and Perimeter Controls) ..... ৪১
৮.৫ নেটওয়ার্ক বিভাজন (Network Segmentation) ..... ৪১
৮.৬ নিরাপদ রিমোট কানেক্টিভিটি (Secure Remote Connectivity) ..... ৪২
৯. এন্ডপয়েন্ট ও ওয়ার্কস্টেশন নিরাপত্তা (Endpoint and Workstation Security) ..... ৪৩
৯.১ লাইসেন্সকৃত সফটওয়্যার ব্যবহার (Licensed Software Enforcement) ..... ৪৩
৯.২ এন্ডপয়েন্ট প্রোটেকশন ও অ্যান্টিভাইরাস (Endpoint Protection and Antivirus) ..... ৪৩
৯.৩ ইউএসবি নিয়ন্ত্রণ (USB Controls) ..... ৪৩
৯.৪ ডিস্ক এনক্রিপশন ও ডেটা সুরক্ষা (Disk Encryption and Data Protection) ..... ৪৪

৯.৫ কেন্দ্রীয় ব্যবস্থাপনা ও ডিরেক্টরি সার্ভিসেস (Centralized Management and Directory Services) ..... ৪৪
১০. সোর্স কোড ও অ্যাপ্লিকেশন নিরাপত্তা (Source Code and Application Security) .৪৫
১০.১ সোর্স কোড মালিকানা ও হেফাজত (Source Code Ownership and Custody) ....৪৫
১০.২ সিকিউর কোডিং গাইডলাইন (Secure Coding Guidelines) ..... ৪৫
১০.৩ ভার্সন কন্ট্রোল ও পরিবর্তন ব্যবস্থাপনা (Version Control and Change Management) ..... ৪৫
১০.৪ কোড রিভিউ ও অনুমোদন প্রক্রিয়া (Code Review and Approval Processes) ....৪৬
কোড লাইভে ডেপ্লয় হওয়ার আগে আনুষ্ঠানিক রিভিউ প্রক্রিয়া থাকতে হবে। ..... ৪৬
১০.৫ কোড রিলিজের নিরাপত্তা পরীক্ষা (Security Testing for Code Releases) ..... ৪৬
১১. ক্লাউড ও ডাটা সেন্টার নিরাপত্তা (Cloud and Data Center Security) ..... ৪৭
১১.১ ক্লাউড শাসন ও কমপ্লায়েন্স (Cloud Governance and Compliance)..... ৪৭
১১.২ ক্লাউড নিরাপত্তা নিয়ন্ত্রণ (Cloud Security Controls) ..... ৪৭
১১.৩ ক্লাউড পর্যবেক্ষণ ও লগ ব্যবস্থাপনা..... ৪৭
১১.৪ ব্যাকআপ ও দুর্যোগ পুনরুদ্ধার..... ৪৮
১১.৫ ক্লাউড ভেন্ডর ব্যবস্থাপনা ..... ৪৮
১২. নিরাপত্তা মনিটরিং ও অপারেশনস (Security Monitoring and Operations) ..... ৪৯
১২.১ SIEM ও লগ ম্যানেজমেন্ট (SIEM and Log Management) ..... ৪৯
১২.২ ইনসিডেন্ট শনাক্তকরণ ও প্রতিক্রিয়া (Incident Detection and Response) ..... ৪৯
১২.৩ এসকেলেশন ম্যাট্রিক্স ও SLA প্রয়োগ (Escalation Matrix and SLA Enforcement) ..... ৫০
১২.৪ ডার্ক ওয়েব মনিটরিং (Dark Web Monitoring) ..... ৫০
১২.৫ নিরাপত্তা সচেতনতা ও প্রশিক্ষণ (Security Awareness and Training) ..... ৫০
১৩. নিরাপত্তা মূল্যায়ন ও টেস্টিং (Security Assessment and Testing)..... ৫১
১৩.১ ভালনারেবিলিটি এসেসমেন্ট ও পেনেট্রেশন টেস্টিং (VAPT) ..... ৫১
১৩.২ নিরাপত্তা টেস্টিং ব্যবস্থাপনা (Security Testing Management)..... ৫২
১৩.৩ টেস্টিংয়ের ফ্রিকোয়েন্সি ও স্কোপ (Testing Frequency and Scope)..... ৫২
১৩.৪ রেমিডিয়েশনের পর টেস্টিং (Post-Remediation Testing) ..... ৫২
১৩.৫ তৃতীয় পক্ষের নিরাপত্তা টেস্টিং শর্ত (Third-Party Security Testing Requirements) ..... ৫৩

১৪. কর্ম-সম্পাদন ধারাবাহিকতা ও দুর্যোগ পুনরুদ্ধার (Business Continuity and Disaster Recovery - BCDR) ..... ৫৪
১৪.১ BCM ও DR ব্যবস্থাপনা (BCM and DR Management) ..... ৫৪
১৪.২ ডেটা ও প্রক্রিয়ার তালিকা (Data and Process Inventory) ..... ৫৪
১৪.৩ RTO/RPO নির্ধারণ (RTO/RPO Definitions) ..... ৫৫
১৪.৪ ব্যাকআপ ব্যবস্থাপনা ও যাচাই (Backup Management and Validation) ..... ৫৫
১৪.৫ DR টেস্টিং ও পরিকল্পনা রক্ষণাবেক্ষণ (DR Testing and Plan Maintenance) ..... ৫৫
১৫. প্রশিক্ষণ ও সচেতনতা (Training and Security Awareness) ..... ৫৭
১৫.১ নিরাপত্তা সচেতনতা ..... ৫৭
১৫.২ আইসিটি কর্মীদের কারিগরি প্রশিক্ষণ ..... ৫৭
১৫.৩ ভেন্ডর প্রশিক্ষণ ..... ৫৭
১৫.৪ মহড়া (Simulation Exercise) ..... ৫৭
১৫.৫ প্রশিক্ষণ রেকর্ড: প্রশিক্ষণ, অংশগ্রহণ, মূল্যায়ন এবং ফলাফল সংক্রান্ত রেকর্ড সংরক্ষণ করতে হবে। ..... ৫৭
১৬. উদীয়মান প্রযুক্তির নিরাপত্তা (Emerging Technology Security) ..... ৫৮
১৬.১ কৃত্রিম বুদ্ধিমত্তা (Artificial Intelligence) ..... ৫৮
১৬.২ Machine Learning ..... ৫৮
১৬.৩ API Security ..... ৫৮
১৬.৪ Internet of Things (IoT) ..... ৫৯
১৬.৫ Robotic Process Automation (RPA) ..... ৫৯
১৬.৬ সামাজিক যোগাযোগ মাধ্যম ও ভার্চুয়াল মিটিং ..... ৫৯
১৬.৭ উদীয়মান প্রযুক্তির ঝুঁকি মূল্যায়ন ..... ৫৯
১৭. কমপ্লায়েন্স, রিপোর্টিং ও নন-কমপ্লায়েন্স ব্যবস্থা (Compliance, Reporting and Non-Compliance Management) ..... ৬০
১৭.১ কমপ্লায়েন্স (Compliance) ..... ৬০
১৭.২ পর্যবেক্ষণ ও রিপোর্টিং (Monitoring and Reporting) ..... ৬০
১৭.৩ নিরাপত্তা ঘটনার রিপোর্টিং ..... ৬০
১৭.৪ যাচাইকরণ (Verification) ..... ৬০
১৭.৫ নন-কমপ্লায়েন্স ব্যবস্থাপনা ..... ৬০
১৭.৬ ব্যতিক্রম অনুমোদন (Exception Management) ..... ৬১
১৭.৭ ধারাবাহিক উন্নয়ন (Continuous Improvement) ..... ৬১

১৮. বিবিধ.....৬১
১৮.১ নির্দেশ প্রদানের ক্ষমতা: .....৬১
১৮.২ অব্যাহতি:.....৬১
১৮.৩ নির্দেশিকার সীমাবদ্ধতা:.....৬১
গুরুত্বপূর্ণ শব্দকোষ এবং সংক্ষিপ্ত রূপ..... ৬২

## ১. ভূমিকা

ভূমি মানুষের জীবনের সঙ্গে নিবিড়ভাবে সম্পর্কিত, যা অস্তিত্ব রক্ষা এবং জীবিকা উপার্জনের মূল ভিত্তি। রাষ্ট্রের দায়িত্ব হলো নাগরিকের ভূমি অধিকার আইনানুগভাবে নিশ্চিত করা, সুরক্ষা প্রদান এবং সেবার সুবিধা সহজতর করা। দেশে ভূমি সেবার ব্যবস্থাপনা দীর্ঘদিন কাগজভিত্তিক হলেও সম্প্রতি ডিজিটালাইজড প্রক্রিয়া চালু হয়েছে, যা নাগরিকদের সেবা গ্রহণ, অগ্রগতি পর্যবেক্ষণ ও ফলাফল প্রাপ্তি সহজতর করে তুলেছে। তবে প্রযুক্তি ভিত্তিক এই সেবা নিরাপদ থাকবে শুধুমাত্র যথাযথ নিরাপত্তা নিশ্চিত করা সম্ভব হলে, যার জন্য প্রয়োজন হার্ডওয়ার, সফ্টওয়ার, নেটওয়ার্ক, তথ্য এবং নিয়োজিত মানুষের উপর সার্বক্ষণিক নজরদারি। ভূমি সেবায় নাগরিক, সরকারি ও বেসরকারি বিভিন্ন সংস্থা যুক্ত থাকায়, প্রতিটি তথ্য এবং তার আন্তঃসম্পর্কিত তথ্য-উপাত্ত নিরাপদভাবে অর্জন, ব্যবস্থাপনা, পর্যবেক্ষণ ও মূল্যায়ন করা অত্যন্ত জরুরি। সরকারের তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ ইতোমধ্যেই এসংক্রান্ত বিভিন্ন আইন, বিধি, নীতি ও নির্দেশিকা জারি করেছে। এসবের সঙ্গে সংগতি রেখে জনবান্ধব ভূমি সেবার জন্য সাইবার নিরাপত্তা ও তথ্য সুরক্ষা নির্দেশিকা প্রণয়ন অপরিহার্য।

### ১.১ শিরোনাম, প্রয়োগ ও প্রবর্তন:

(১) এ নির্দেশিকা “ভূমিসেবায় সাইবার নিরাপত্তা ও তথ্য সুরক্ষা নির্দেশিকা” হিসেবে অবিহিত হবে

(২) এ নির্দেশিকার বিধানাবলি ভূমি মন্ত্রণালয় ও এর আওতাধীন দপ্তরের সকল কর্মকর্তা/কর্মচারী, প্রকল্প/কর্মসূচি এবং পরামর্শক/ভেন্ডর প্রতিষ্ঠান যারা প্রত্যক্ষ বা পরোক্ষভাবে ভূমিসেবার সাথে সংশ্লিষ্টদের ক্ষেত্রে প্রয়োগ হবে।

(৩) ভূমি মন্ত্রণালয়, আদেশ দ্বারা, যে তারিখ নির্ধারণ করবে সে তারিখ হতে এ নির্দেশিকা কার্যকর হবে।

### ১.২ সংজ্ঞা:

(১) বিষয় বা প্রসঙ্গের পরিপন্থি কোনো কিছু না থাকলে, এই নির্দেশিকায়

(ক) “আক্রম্যতা (Vulnerability)" অর্থ কম্পিউটার সিস্টেমের দুর্বলতা, যার সুযোগ গ্রহণ করে উক্ত সিস্টেমের বিশ্বস্ততা বা গোপনীয়তা (Confidentiality), অখণ্ডতা বা শুদ্ধতা (Integrity) এবং লভ্যতাকে (Availability) নেতিবাচকভাবে প্রভাবিত করা যায়;

(খ) “তথ্য প্রযুক্তি” অর্থ পরস্পর সংযুক্ত এমন একটি ব্যবস্থা যাতে তথ্যে প্রবেশগম্যতাসহ তথ্য সংরক্ষণ, প্রক্রিয়াজাতকরণ ও বিশ্লেষণ বা প্রেরণ করা হয়;

(গ) “দুর্যোগ পুনরুদ্ধার পরিকল্পনা (Disaster Recovery Planning)” অর্থ তথ্য প্রযুক্তি বা কম্পিউটার সিস্টেম ব্যাহত হবার ক্ষেত্রে যে পদ্ধতিতে এর সক্ষমতা পুনরুদ্ধার করা হয়;

(ঘ) “দূর নিয়ন্ত্রণ প্রবেশ (Remote Access)” অর্থ কোনো ব্যবহারকারী কর্তৃক বহিঃস্থ নেটওয়ার্ক যোগাযোগের মাধ্যমে তথ্য প্রযুক্তির পরিকাঠামোতে প্রবেশ;

(ঙ) “নেটওয়ার্ক নিরাপত্তা (Network Security)” অর্থ কম্পিউটার নেটওয়ার্ক বা কম্পিউটার সিস্টেমের নিরাপত্তা;

(চ) “নেটওয়ার্ক জোন” অর্থ কম্পিউটার নেটওয়ার্কের যৌক্তিকভাবে বিভাজিত অংশ;

(ছ) “প্যাচ” অর্থ বিশেষ ধরনের প্রোগ্রাম যাহা সফটওয়্যার অথবা অপারেটিং সিস্টেমের চিহ্নিত ঘাটতি বা সীমাবদ্ধতা দূর করে প্রোগ্রামের কার্যকারিতা, ব্যবহারযোগ্যতা বা কর্মক্ষমতা উন্নত করে;

(জ) “ভ্যালনারেবিলিটি অ্যাসেসমেন্ট” অর্থ সিস্টেম, নেটওয়ার্ক বা অ্যাপ্লিকেশনে থাকা নিরাপত্তার দুর্বলতা চিহ্নিত, মূল্যায়ন ও ডকুমেন্ট করার প্রক্রিয়া।

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

(ঞ) “সিকিউরিটি বেইজলাইন কনফিগারেশন স্ট্যান্ডার্ড” অর্থ তথ্য প্রযুক্তির বা অপারেশন প্রযুক্তির জন্য লিখিত প্রক্ষেপণমালা যা কোনো এক সময় আনুষ্ঠানিকভাবে স্বীকৃত হইয়াছে;

(২) এই নির্দেশিকায় ব্যবহৃত যে সকল শব্দ বা অভিব্যক্তির সংজ্ঞা এই নির্দেশিকায় প্রদান করা হয়নি, সে সকল শব্দ বা অভিব্যক্তি আইন, বিধিমালা ও তথ্য ও যোগাযোগ প্রযুক্তি আইন-২০০৬, জাতীয় উপাত্ত ব্যবস্থাপনা আইন-২০২৬, ব্যক্তিগত উপাত্ত সুরক্ষা আইন-২০২৬, সাইবার সুরক্ষা আইন-২০২৬ এ যে অর্থে ব্যবহৃত হয়েছে সে অর্থে প্রযোজ্য হবে।

### ১.৩ লক্ষ্য

ভূমিসেবায় সাইবার নিরাপত্তা ও তথ্য সুরক্ষা নির্দেশিকার মূল লক্ষ্য হলো ভূমি এবং ভূমিসেবা সংক্রান্ত তথ্য-উপাত্ত ও সিস্টেমের গোপনীয়তা (Confidentiality), অখন্ডতা বা শুদ্ধতা (Integrity) ও লভ্যতা (Availability)-কে সুরক্ষা কবচ দ্বারা আবদ্ধ রাখাসহ সাইবার হুমকি মোকাবেলা এবং ঝুঁকি ব্যবস্থাপনায় সুশাসন প্রতিষ্ঠার মাধ্যমে বিশ্বাসযোগ্য ও মানসম্মত ভূমিসেবা নিশ্চিতকরা। এটি ঝুঁকি ব্যবস্থাপনায় সক্রিয় পদক্ষেপ নেওয়া, জাতীয় ও আন্তর্জাতিক মানদন্ড মেনে চলা এবং তথ্য নিরাপত্তা চর্চার ধারাবাহিক উন্নয়ন নিশ্চিত করার সংস্কৃতি গড়ে তুলতে সাহায্য করবে।

## ১.৪ পরিধি (Scope)

এই নির্দেশিকা ভূমি মন্ত্রণালয় ও এর আওতাধীন দপ্তরের সব ধরনের আইসিটি অবকাঠামো, সিস্টেম, অ্যাপ্লিকেশন, তথ্য-উপাত্ত পরিসম্পদ, কর্মী এবং এতদসংক্রান্ত কাজে যুক্ত পরামর্শক/ভেন্ডর প্রতিষ্ঠানের জন্য প্রযোজ্য। এটি নিচের বিষয়গুলোকে অন্তর্ভুক্ত করে-

১. নাগরিক ও প্রশাসনিক সেবা প্রদানের জন্য ব্যবহৃত সফ্টওয়্যার, ওয়েবসাইট ও মোবাইল অ্যাপ্লিকেশন;

২. ভূমি মন্ত্রণালয় ও এর আওতাধীন দপ্তরের অভ্যন্তরীণ সিস্টেম যেমন সার্ভার, ডেটাবেস, ওয়ার্কস্টেশন ও নেটওয়ার্ক উপাদান;

৩. তৃতীয় পক্ষের পরামর্শক/ভেন্ডর প্রতিষ্ঠান দ্বারা পরিচালিত সফটওয়্যার উন্নয়ন, রক্ষণাবেক্ষণ ও বাস্তবায়ন কার্যক্রম এবং যেকোনো ডেটা প্রক্রিয়াকরণ কার্যক্রম;

৪. বিভিন্ন গুরুত্বপূর্ণ কার্যক্রম সংশ্লিষ্ট বিষয় যেমন: প্রবেশাধিকার নিয়ন্ত্রণ (Access Control), এন্ডপয়েন্ট সিকিউরিটি (End Point Security), পরিবীক্ষণ (Monitoring), ঘটনার প্রতিক্রিয়া (Incident Response), কর্ম-সম্পাদন ধারাবাহিকতা (Business Continuity) ও দুর্যোগ পুনরুদ্ধার (Disaster Recovery);

## ১.৫ প্রযোজ্যতা (Applicability)

এই নির্দেশিকা প্রযোজ্য হবে-

১. ভূমি মন্ত্রণালয় ও এর আওতাধীন দপ্তরের সকল কর্মকর্তা/কর্মচারী, প্রকল্প/কর্মসূচি এবং পরামর্শক/ভেন্ডর প্রতিষ্ঠান যারা প্রত্যক্ষ বা পরোক্ষভাবে ভূমিসেবার সাথে সংশ্লিষ্ট;

২. সকল পরামর্শক/ভেন্ডর প্রতিষ্ঠান যাদের ভূমি মন্ত্রণালয়ের সিস্টেম বা ডেটায় প্রবেশাধিকার বিদ্যমান;

৩. মন্ত্রণালয়ের সমস্ত আইসিটি সিস্টেম, তা নিজস্ব সার্ভারে হোস্ট করা হোক, প্রাইভেট বা পাবলিক ক্লাউডে হোক, অথবা ন্যাশনাল ডাটা সেন্টারে হোস্ট করা হোক;

৪. মন্ত্রণালয়ের পক্ষে 'গোপনীয় (Confidential)' বা 'শুধুমাত্র অভ্যন্তরীণ ব্যবহারের জন্য (Internal Use)' শ্রেণিভুক্ত তথ্য পরিচালনা করা কোনো বাহ্যিক পক্ষ।

প্রত্যেক সংশ্লিষ্ট পক্ষকে এই নির্দেশিকায় বর্ণিত নির্দেশনা ও নিরাপত্তা ব্যবস্থা যথাযথভাবে অনুসরণ করতে হবে। কোনো ব্যত্যয় বা লঙ্ঘন সংঘটিত হলে তার গুরুত্ব অনুযায়ী প্রয়োজনীয় প্রশাসনিক বা আইনগত ব্যবস্থা গ্রহণ করা হবে।

## ১.৬. আইনগত ভিত্তি

১. জাতীয় উপাত্ত ব্যবস্থাপনা আইন, ২০২৬

২. ব্যক্তিগত উপাত্ত সুরক্ষা আইন, ২০২৬

৩. সাইবার সুরক্ষা আইন, ২০২৬

৪. তথ্য ও যোগাযোগ প্রযুক্তি (সংশোধন) আইন, ২০১৩

৫. তথ্য ও যোগাযোগ প্রযুক্তি (সংশোধন) আইন, ২০০৯

৬. তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬

৭. গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা সুরক্ষা গাইডলাইন ২০২২

৮. Government of Bangladesh Information Security Manual

৯. বাংলাদেশ ন্যাশনাল ডিজিটাল আর্কিটেকচার (BNDA) নির্দেশিকা

১০. Secure Coding Guidelines

১১. তথ্য নিরাপত্তা পলিসি গাইডলাইন

১২. ভূমি ব্যবস্থাপনা সংক্রান্ত সকল আইন/বিধি/নীতিমালা/নির্দেশিকা/পরিপত্র

## ১.৭ রেফারেন্স ও মানদণ্ড (References and Standards)

এই নির্দেশিকাটি আন্তর্জাতিকভাবে স্বীকৃত কিছু মান ও ফ্রেমওয়ার্কের সঙ্গে সামঞ্জস্য রেখে প্রণয়ন করা হয়েছে যেন উত্তম চর্চা নিশ্চিত করা সম্ভব হয়, যার মধ্যে রয়েছে-

১. ISO/IEC ২৭০০১:২০২২ - International standard for Information Security Management Systems (ISMS) একটি আন্তর্জাতিক মানদণ্ড, যা প্রতিষ্ঠানের তথ্য নিরাপত্তা ব্যবস্থাপনার জন্য কাঠামো, নিয়ন্ত্রণ এবং প্রক্রিয়া নির্ধারণ করে।

২. National Institute of Standards and Technology (NIST) Cybersecurity Framework - যুক্তরাষ্ট্রের ন্যাশনাল ইনস্টিটিউট অব স্ট্যান্ডার্ডস অ্যান্ড টেকনোলজি কর্তৃক প্রণীত সাইবার সিকিউরিটি শাসন কাঠামো, যা প্রতিষ্ঠানগুলোকে তাদের সাইবার নিরাপত্তা ব্যবস্থাপনা উন্নত করতে সাহায্য করে।

৩. Open Web Application Security Project (OWASP) Secure Coding Practices - নিরাপদ সফ্টওয়্যার ডেভেলপমেন্টের জন্য একটি রেফারেন্স মডেল বা নির্দেশিকা, যা ডেভেলপারদের নিরাপদ কোড লিখতে সহায়তা করে এবং সফ্টওয়্যার/ওয়েব অ্যাপ্লিকেশনকে হ্যাকিং ও নিরাপত্তাজনিত ঝুঁকি থেকে রক্ষা করে।

৪. Information Systems Audit and Control Association (ISACA) IT Assurance Framework (ITAF) - আইটি অডিট, নিয়ন্ত্রণ ও নিরাপত্তা কার্যক্রমে মান নিশ্চিত করতে সাহায্য করে এবং ঝুঁকি ও দুর্বলতা চিহ্নিত করার জন্য নির্দেশিকা প্রদান করে।

এই মানদণ্ডগুলো মন্ত্রণালয়ের তথ্য নিরাপত্তা ব্যবস্থার উন্নয়ন, বাস্তবায়ন, রক্ষণাবেক্ষণ এবং ধারাবাহিক উন্নতির দিকনির্দেশনা প্রদান করে।

## ২. শাসন ও নিরাপত্তা ব্যবস্থাপনা (Governance and Security Management)

### ২.১ তথ্য নিরাপত্তা নীতি (Information Security Policy)

ভূমি মন্ত্রণালয়ের তথ্য-উপাত্ত, তথ্যপ্রযুক্তি অবকাঠামো এবং ডিজিটাল সেবার গোপনীয়তা (Confidentiality), অখণ্ডতা (Integrity) ও লভ্যতা (Availability) নিশ্চিত করার লক্ষ্যে তথ্য নিরাপত্তা ব্যবস্থাপনায় নিম্নোক্ত বিষয়সমূহ অনুসরণ করতে হবে-

১. তথ্য সম্পদের গোপনীয়তা, অখণ্ডতা ও লভ্যতা (CIA) নিশ্চিত করতে হবে;
২. তথ্য নিরাপত্তা ব্যবস্থাপনা মন্ত্রণালয়ের কৌশলগত লক্ষ্য, আইন, বিধি এবং সেবার চাহিদার সঙ্গে সামঞ্জস্যপূর্ণ হতে হবে;
৩. তথ্য-উপাত্ত পরিচালনাকারী ও ব্যবহারকারী সকল কর্মকর্তা/কর্মচারী, প্রকল্প, পরামর্শক, ভেন্ডর এবং তৃতীয় পক্ষ এই নির্দেশিকায় বর্ণিত নিরাপত্তা ব্যবস্থা অনুসরণ করবেন;
৪. প্রবেশাধিকার নিয়ন্ত্রণ (Access Control), সম্পদ ব্যবস্থাপনা (Asset Management), তথ্য শ্রেণিবিন্যাস (Data Classification), তথ্য পরিচালনা (Data Handling), ঘটনার প্রতিক্রিয়া (Incident Response), এন্ডপয়েন্ট নিরাপত্তা (Endpoint Security), কর্ম-সম্পাদনের ধারাবাহিকতা (Business Continuity), দুর্যোগ পুনরুদ্ধার (Disaster Recovery), লগ ব্যবস্থাপনা (Log Management) এবং ঝুঁকি ব্যবস্থাপনার জন্য প্রয়োজনীয় নিরাপত্তা ব্যবস্থা বাস্তবায়ন করতে হবে;
৫. তথ্য নিরাপত্তা ব্যবস্থাপনার কার্যকর বাস্তবায়নের জন্য প্রয়োজনীয় Standard Operating Procedure (SOP), কারিগরি মানদণ্ড (Technical Standards), নির্দেশিকা (Guidelines), বেইজলাইন কনফিগারেশন (Baseline Configuration), চেকলিস্ট (Checklist) এবং প্রয়োজনীয় ফরম (Forms/Templates) প্রণয়ন, হালনাগাদ ও অনুসরণ করতে হবে;
৬. তথ্য নিরাপত্তা ব্যবস্থা কমপক্ষে বছরে একবার অথবা গুরুত্বপূর্ণ প্রযুক্তিগত, আইনগত বা সাংগঠনিক পরিবর্তনের পর পর্যালোচনা করতে হবে;
৭. এই নির্দেশিকার বাস্তবায়ন সম্পর্কে সকল সংশ্লিষ্ট ব্যক্তিকে অবহিত করতে হবে এবং প্রয়োজনীয় সচেতনতা ও প্রশিক্ষণের ব্যবস্থা করতে হবে।

#### ২.১.১ স্ট্যান্ডার্ড অপারেটিং প্রসিডিউর (Standard Operating Procedures)

এই নির্দেশিকার কার্যকর বাস্তবায়ন নিশ্চিত করার লক্ষ্যে তথ্য নিরাপত্তা ব্যবস্থাপনার বিভিন্ন কার্যক্রমের জন্য প্রয়োজনীয় স্ট্যান্ডার্ড অপারেটিং প্রসিডিউর (Standard Operating Procedure - SOP) প্রণয়ন, অনুমোদন, বাস্তবায়ন, হালনাগাদ এবং অনুসরণ করতে হবে। প্রতিটি SOP-এ সংশ্লিষ্ট কার্যক্রমের উদ্দেশ্য, পরিধি, দায়িত্ব, অনুমোদনকারী কর্তৃপক্ষ, কার্যসম্পাদনের ধাপ, নিরাপত্তা নিয়ন্ত্রণ, রেকর্ড সংরক্ষণ এবং পর্যালোচনার পদ্ধতি সুস্পষ্টভাবে উল্লেখ থাকতে হবে।

#### *ক) SOP-এর সাধারণ নির্দেশনা*

১. প্রতিটি SOP সংশ্লিষ্ট দায়িত্বপ্রাপ্ত ইউনিট কর্তৃক প্রণীত হবে এবং যথাযথ কর্তৃপক্ষ কর্তৃক অনুমোদিত হতে হবে।

২. সকল কর্মকর্তা/কর্মচারী, প্রকল্প, পরামর্শক, ভেন্ডর এবং তৃতীয় পক্ষকে তাদের দায়িত্ব অনুযায়ী প্রযোজ্য SOP অনুসরণ করতে হবে।
৩. কোনো গুরুত্বপূর্ণ প্রযুক্তিগত, আইনগত, সাংগঠনিক বা ব্যবসায়িক পরিবর্তন ঘটলে অথবা কমপক্ষে প্রতি **০২ (দুই) বছর** অন্তর SOP পর্যালোচনা ও প্রয়োজন অনুযায়ী হালনাগাদ করতে হবে।
৪. প্রত্যেক SOP-এর সর্বশেষ অনুমোদিত সংস্করণ (Version) সংরক্ষণ করতে হবে এবং পুরাতন সংস্করণ সংরক্ষণ ও প্রত্যাহারের জন্য Version Control অনুসরণ করতে হবে।
৫. SOP-এর আওতায় সম্পাদিত কার্যক্রমের প্রয়োজনীয় নথি, লগ, অনুমোদনপত্র ও অন্যান্য রেকর্ড নির্ধারিত সময় পর্যন্ত সংরক্ষণ করতে হবে।

### *খ) প্রণয়নযোগ্য SOP-এর ন্যূনতম তালিকা*

ভূমি মন্ত্রণালয়ের তথ্য নিরাপত্তা ব্যবস্থাপনার জন্য প্রয়োজন অনুযায়ী নিম্নোক্ত বা সমজাতীয় SOP প্রণয়ন ও বাস্তবায়ন করতে হবে-

১. ব্যবহারকারী ও প্রবেশাধিকার ব্যবস্থাপনা (User and Access Management SOP)
২. পাসওয়ার্ড ব্যবস্থাপনা (Password Management SOP)
৩. তথ্য সম্পদ ব্যবস্থাপনা (Asset Management SOP)
৪. তথ্য শ্রেণিবিন্যাস ও তথ্য পরিচালনা (Data Classification and Data Handling SOP)
৫. ব্যাকআপ ও পুনরুদ্ধার (Backup and Restore SOP)
৬. দুর্যোগ পুনরুদ্ধার ও ব্যবসায়িক ধারাবাহিকতা (Disaster Recovery and Business Continuity SOP)
৭. নিরাপত্তা ঘটনা ব্যবস্থাপনা (Security Incident Response SOP)
৮. পরিবর্তন ব্যবস্থাপনা (Change Management SOP)
৯. ভ্যালনারেবিলিটি মূল্যায়ন, প্যাচ ও নিরাপত্তা হালনাগাদ ব্যবস্থাপনা (Vulnerability Assessment, Patch and Security Update Management SOP)
১০. লগ পর্যবেক্ষণ ও নিরাপত্তা পর্যবেক্ষণ (Log Monitoring and Security Monitoring SOP)
১১. দূরবর্তী প্রবেশাধিকার ব্যবস্থাপনা (Remote Access Management SOP)
১২. তৃতীয় পক্ষ ও ভেন্ডর নিরাপত্তা ব্যবস্থাপনা (Third-Party and Vendor Security Management SOP)
১৩. নিরাপদ সফটওয়্যার উন্নয়ন জীবনচক্র (Secure Software Development Life Cycle - SSDLC SOP)
১৪. ক্লাউড ও ডাটা সেন্টার পরিচালনা (Cloud and Data Center Operations SOP)
১৫. GIS, Geospatial ও ভূমি তথ্য নিরাপত্তা (GIS and Land Information Security SOP)
১৬. ডিজিটাল তথ্য সংরক্ষণ, আর্কাইভিং ও নিরাপদ অপসারণ (Data Retention, Archiving and Secure Disposal SOP)
১৭. ক্রিপ্টোগ্রাফিক কী ব্যবস্থাপনা (Cryptographic Key Management SOP)

১৮. তথ্য নিরাপত্তা সচেতনতা ও প্রশিক্ষণ (Information Security Awareness and Training SOP)

### গ) SOP-*এর ন্যূনতম কাঠামো*

প্রতিটি SOP-এ অন্তত নিম্নোক্ত বিষয়সমূহ অন্তর্ভুক্ত থাকতে হবে-

১. উদ্দেশ্য (Purpose)
২. পরিধি (Scope)
৩. প্রযোজ্যতা (Applicability)
৪. দায়িত্ব ও কর্তৃত্ব (Roles and Responsibilities)
৫. কার্যসম্পাদনের ধাপ (Procedures)
৬. নিরাপত্তা নিয়ন্ত্রণ (Security Controls)
৭. প্রয়োজনীয় ফরম, চেকলিস্ট ও রেকর্ড (Forms, Checklists and Records)
৮. ব্যতিক্রম ব্যবস্থাপনা (Exception Handling)
৯. রেফারেন্স (References)
১০. পর্যালোচনা ও সংস্করণ নিয়ন্ত্রণ (Review and Version Control)

### ঘ) SOP-*এর বাস্তবায়ন ও তদারকি*

সংশ্লিষ্ট ইউনিট প্রধান এবং তথ্য নিরাপত্তা ব্যবস্থাপনার দায়িত্বপ্রাপ্ত কর্মকর্তা (CISO/ISO) প্রযোজ্য SOP-এর বাস্তবায়ন, কার্যকারিতা এবং প্রতিপালন নিয়মিত পর্যবেক্ষণ করবেন। SOP অনুসরণে কোনো ব্যত্যয় পরিলক্ষিত হলে প্রয়োজনীয় সংশোধনমূলক ব্যবস্থা গ্রহণ করতে হবে এবং প্রয়োজনে সংশ্লিষ্ট কর্তৃপক্ষকে অবহিত করতে হবে। প্রয়োজন অনুযায়ী প্রতিটি SOP বাস্তবায়নের সহায়ক হিসেবে কারিগরি মানদণ্ড (Technical Standards), বেইজলাইন কনফিগারেশন (Baseline Configuration), নির্দেশনা (Guidelines), চেকলিস্ট (Checklists) এবং প্রয়োজনীয় ফরম (Forms/Templates) প্রণয়ন ও ব্যবহার করতে হবে।

## ২.২ ভূমিকা ও দায়িত্ব (Roles and Responsibilities)

কার্যকর তথ্য নিরাপত্তা শাসনব্যবস্থা (Information Security Governance) নিশ্চিত করার লক্ষ্যে তথ্য ও যোগাযোগ প্রযুক্তি (ICT) সম্পদ, তথ্য-উপাত্ত এবং সংশ্লিষ্ট সেবাসমূহের নিরাপত্তা ব্যবস্থাপনায় সম্পৃক্ত সকল ব্যক্তি, ইউনিট ও অংশীজনের দায়িত্ব সুস্পষ্টভাবে নির্ধারণ করতে হবে। দায়িত্ব বণ্টনের ক্ষেত্রে জবাবদিহিতা (Accountability), দায়িত্বের পৃথকীকরণ (Segregation of Duties), প্রয়োজনীয় ক্ষমতা (Authority) এবং সমন্বিত তদারকি নিশ্চিত করতে হবে।

ক) সিনিয়র ম্যানেজমেন্ট (Senior Management)

সিনিয়র ম্যানেজমেন্ট তথ্য নিরাপত্তা ব্যবস্থাপনার সর্বোচ্চ নীতিনির্ধারণী কর্তৃপক্ষ হিসেবে দায়িত্ব পালন করবে।

**ব্যবস্থাপনা কমিটির গঠন (Information Security Governance Committee):**

১. সিনিয়র সচিব/সচিব - সভাপতি
২. অতিরিক্ত সচিব/যুগ্ম সচিব (প্রশাসন ও অর্থ) - সদস্য
৩. অতিরিক্ত সচিব/যুগ্ম সচিব (ডিকেএমপি) - সদস্য
৪. CISO/ISO - সদস্য সচিব
    - প্রয়োজনে সংশ্লিষ্ট সিস্টেমের মালিক (System Owner), প্রকল্প পরিচালক, প্রধান হিসাব ও অর্থ কর্মকর্তা, আইটি অপারেশনস ও সিকিউরিটি টিমের প্রতিনিধি অথবা অন্য কোনো বিশেষজ্ঞকে সভায় আমন্ত্রণ জানানো যাবে।

**দায়িত্ব:**

১. তথ্য নিরাপত্তা, সাইবার নিরাপত্তা ও তথ্য সুরক্ষা নীতি, নির্দেশিকা, মানদণ্ড ও সংশ্লিষ্ট কার্যপদ্ধতি অনুমোদন, প্রয়োজন অনুযায়ী সংশোধন এবং কমপক্ষে বছরে একবার বা গুরুত্বপূর্ণ পরিবর্তনের পর পর্যালোচনা করা।

২. প্রয়োজনীয় বাজেট, জনবল, প্রযুক্তি ও অন্যান্য সম্পদ বরাদ্দ নিশ্চিত করা।

৩. প্রতিষ্ঠানের তথ্য নিরাপত্তা ঝুঁকি (Cyber Risk) গ্রহণ, হ্রাস অথবা প্রশমনের বিষয়ে সিদ্ধান্ত গ্রহণ করা।

৪. জাতীয় আইন, বিধি, নীতি এবং আন্তর্জাতিক মানদণ্ড অনুসরণ নিশ্চিত করা।

৫. গুরুত্বপূর্ণ সাইবার নিরাপত্তা ঘটনা (Major Cyber Security Incident), ঝুঁকি মূল্যায়ন, নিরীক্ষা (Audit) ও কমপ্লায়েন্স প্রতিবেদন নিয়মিত পর্যালোচনা করে প্রয়োজনীয় নীতিগত সিদ্ধান্ত গ্রহণ, নির্দেশনা প্রদান এবং সংশোধনমূলক কার্যক্রমের বাস্তবায়ন নিশ্চিত করা।

৬. ব্যবসায়িক ধারাবাহিকতা (Business Continuity) ও দুর্যোগ পুনরুদ্ধার (Disaster Recovery) কার্যক্রমের জন্য প্রয়োজনীয় নীতিগত সিদ্ধান্ত গ্রহণ করা।

৭. তথ্য নিরাপত্তা কর্মসম্পাদন সূচক (Security KPIs), গুরুত্বপূর্ণ ঝুঁকি সূচক (KRIs), কমপ্লায়েন্স অবস্থা এবং নিরাপত্তা নিয়ন্ত্রণের কার্যকারিতা নিয়মিত পর্যালোচনা করা।

৮. তথ্য নিরাপত্তা সংস্কৃতি (Security Culture) প্রতিষ্ঠা এবং সকল পর্যায়ে নিরাপত্তা বিষয়ে জবাবদিহিতা নিশ্চিত করা।

## খ) CISO/ISO (Chief Information Security Officer/Information Security Officer):

CISO/ISO প্রতিষ্ঠানের তথ্য নিরাপত্তা ব্যবস্থাপনার কেন্দ্রীয় সমন্বয়কারী এবং নিরাপত্তা শাসন বাস্তবায়নের জন্য দায়িত্বপ্রাপ্ত কর্মকর্তা।

**দায়িত্ব:**

১. তথ্য নিরাপত্তা নীতি, মানদণ্ড, নিয়ন্ত্রণ ব্যবস্থা (Security Controls) ও নির্দেশিকা প্রণয়ন, বাস্তবায়ন এবং নিয়মিত হালনাগাদ করা।
২. তথ্য নিরাপত্তা ঝুঁকি মূল্যায়ন (Risk Assessment), ঝুঁকি ব্যবস্থাপনা (Risk Treatment) এবং ঝুঁকি নিবন্ধন (Risk Register) পরিচালনা করা।
৩. নিরাপত্তা পর্যবেক্ষণ, কমপ্লায়েন্স মূল্যায়ন, অভ্যন্তরীণ অডিট এবং সংশোধনমূলক কার্যক্রম সমন্বয় করা।
৪. তথ্য নিরাপত্তা ঘটনা (Security Incident) ব্যবস্থাপনা, তদন্ত, রিপোর্টিং এবং প্রয়োজনীয় কর্তৃপক্ষের সাথে সমন্বয় করা।
৫. তৃতীয় পক্ষ, ভেন্ডর ও ক্লাউড সেবা প্রদানকারীদের নিরাপত্তা সম্মতি (Security Compliance) নিশ্চিত করা।
৬. নিরাপত্তা সচেতনতা, প্রশিক্ষণ ও মহড়া (Cyber Drill/Table-top Exercise) আয়োজন করা।
৭. প্রয়োজন অনুযায়ী জাতীয় সাইবার নিরাপত্তা সংস্থা, সরকারি CERT/CIRT এবং সংশ্লিষ্ট কর্তৃপক্ষের সাথে সমন্বয় করা।
৮. নিরাপত্তা কর্মক্ষমতা সূচক (Security Metrics/KPI) প্রস্তুত করে সিনিয়র ম্যানেজমেন্টকে নিয়মিত প্রতিবেদন প্রদান করা।

**দায়িত্বপ্রাপ্ত কর্মকর্তা:**

- মন্ত্রণালয়ের সিস্টেম ম্যানেজার এ দায়িত্ব পালন করবেন। তাঁর অনুপস্থিতিতে নিরাপত্তা ব্যবস্থাপনার দায়িত্বে নিয়োজিত সিনিয়র সিস্টেম এনালিস্ট দায়িত্ব পালন করবেন।

গ) ব্যক্তিগত উপাত্ত সুরক্ষা দায়িত্বপ্রাপ্ত কর্মকর্তা **(Data Protection/Privacy Officer)**

দায়িত্ব:

১. ব্যক্তিগত ও সংবেদনশীল উপাত্তের সংগ্রহ, ব্যবহার, সংরক্ষণ, আদান-প্রদান এবং অপসারণ সংশ্লিষ্ট আইন, বিধি ও নীতিমালার প্রতিপালন নিশ্চিত করা।
২. ব্যক্তিগত উপাত্ত প্রক্রিয়াকরণ কার্যক্রমের ওপর প্রয়োজনীয় তদারকি ও পরামর্শ প্রদান করা।
৩. ব্যক্তিগত উপাত্ত সংক্রান্ত অভিযোগ, তথ্য ফাঁস (Personal Data Breach) এবং গোপনীয়তা-সংক্রান্ত ঘটনাসমূহে CISO/ISO-এর সঙ্গে সমন্বয় করা।
৪. প্রয়োজন অনুযায়ী Privacy Impact Assessment (PIA) বা সমজাতীয় মূল্যায়ন কার্যক্রমে অংশগ্রহণ করা।

**দায়িত্বপ্রাপ্ত কর্মকর্তা:**

- ব্যক্তিগত উপাত্ত সুরক্ষা আইন বা সরকারি নির্দেশনা অনুযায়ী মনোনীত কর্মকর্তা Data Protection Officer (DPO)-এর দায়িত্ব পালন করবেন। এ ধরনের মনোনয়ন না হওয়া পর্যন্ত মন্ত্রণালয় কর্তৃক মনোনীত সিনিয়র সিস্টেম এনালিস্ট এ দায়িত্ব পালন করবেন এবং

তাঁর অনুপস্থিতিতে নিরাপত্তা ব্যবস্থাপনার দায়িত্বে নিয়োজিত সিস্টেম এনালিস্ট দায়িত্ব পালন করবেন।

### ঘ) আইটি অপারেশনস ও সিকিউরিটি টিম (IT Operations and Security Team)

দায়িত্ব:

১. নেটওয়ার্ক, সার্ভার, ক্লাউড, ডাটাবেজ এবং এন্ডপয়েন্ট নিরাপত্তা নিশ্চিত করা।

২. Firewall, IDS/IPS, WAF, SIEM, EDR/XDR, Antivirus, Email Security এবং অন্যান্য নিরাপত্তা নিয়ন্ত্রণ পরিচালনা করা।

৩. নিরাপত্তা লগ পর্যবেক্ষণ, বিশ্লেষণ ও সংরক্ষণ করা।

৪. Vulnerability Assessment, Penetration Testing (VAPT), Secure Configuration, Configuration Baseline Management এবং Patch Management পরিচালনা করা।

৫. Backup, Disaster Recovery এবং Business Continuity Plan বাস্তবায়ন ও নিয়মিত পরীক্ষা করা।

৬. নিরাপত্তা ঘটনার প্রাথমিক প্রতিক্রিয়া (Incident Response), ফরেনসিক তথ্য সংরক্ষণ এবং পুনরুদ্ধার কার্যক্রম পরিচালনা করা।

৭. নিরাপত্তা কনফিগারেশন পরিবর্তনের ক্ষেত্রে অনুমোদিত Change Management অনুসরণ করা।

৮. সকল নিরাপত্তা কার্যক্রমের ডকুমেন্টেশন সংরক্ষণ করা।

**দায়িত্বপ্রাপ্ত কর্মকর্তা:**

- মন্ত্রণালয়ের নিরাপত্তা ব্যবস্থাপনার দায়িত্বে নিয়োজিত সিনিয়র সিস্টেম এনালিস্ট এ কার্যক্রমের সমন্বয় করবেন।

### ঙ) সিস্টেমের মালিক ও তথ্য সম্পদের সংরক্ষক (System Owner and Information Asset Custodian)

**দায়িত্ব:**

১. তথ্য সম্পদের মালিকানা, শ্রেণিবিন্যাস এবং গ্রহণযোগ্য ব্যবহার (Acceptable Use) নিশ্চিত করা।

২. তথ্যের গোপনীয়তা, অখণ্ডতা ও প্রাপ্যতা (Confidentiality, Integrity and Availability) নিশ্চিত করা।

৩. ব্যবহারকারীর প্রবেশাধিকার (Access Rights) অনুমোদন, পরিবর্তন ও প্রত্যাহার করা।

৪. Least Privilege এবং Need-to-Know পদ্ধতি অনুসরণ ও তা বাস্তবায়ন করা।

৫. তথ্য সংরক্ষণ, সংরক্ষণকাল (Retention) এবং নিরাপদ ধ্বংস (Secure Disposal) নিশ্চিত করা।

৬. নিয়মিতভাবে ব্যবহারকারীর প্রবেশাধিকার পর্যালোচনা করা।

৭. নিরাপত্তা ঘটনার ক্ষেত্রে CISO/ISO-এর সাথে সমন্বয় করা।

**দায়িত্বপ্রাপ্ত কর্মকর্তা:**

- মন্ত্রণালয়ের সংশ্লিষ্ট সিস্টেম এনালিস্ট অথবা সংশ্লিষ্ট সিস্টেমের দায়িত্বপ্রাপ্ত কর্মকর্তা এ দায়িত্ব পালন করবেন।

চ) সিস্টেম/অ্যাপ্লিকেশন ডেভেলপার, পরামর্শক, ভেন্ডর ও ঠিকাদার প্রতিষ্ঠান:

**দায়িত্ব:**

১. চুক্তি, NDA, SLA এবং মন্ত্রণালয়ের তথ্য নিরাপত্তা নির্দেশিকা অনুসরণ করা।

২. Secure Software Development Lifecycle (SSDLC) অনুসরণ করা।

৩. Secure Coding Standards এবং OWASP Secure Coding Guidelines অনুসরণ করা।

৪. সফটওয়্যার প্রকাশের পূর্বে নিরাপত্তা পরীক্ষা (Security Testing) সম্পন্ন করা।

৫. Source Code, System Documentation, API Documentation, Configuration, Change Log এবং Security Test Report হস্তান্তর করা।

৬. নিরাপত্তা দুর্বলতা শনাক্ত হলে নির্ধারিত সময়ের মধ্যে সংশোধন করা।

৭. অনুমোদন ছাড়া মন্ত্রণালয়ের তথ্য সংগ্রহ, সংরক্ষণ, কপি, স্থানান্তর অথবা প্রকাশ না করা।

৮. নিরাপত্তা ঘটনার বিষয়ে তাৎক্ষণিকভাবে CISO/ISO-কে অবহিত করা।

ছ) সকল কর্মকর্তা/কর্মচারী প্রতিষ্ঠান:

**দায়িত্ব:**

১. তথ্য নিরাপত্তা নীতি, নির্দেশিকা ও স্ট্যান্ডার্ড অপারেটিং প্রসিডিউর (SOP) অনুসরণ করা।

২. শক্তিশালী পাসওয়ার্ড, মাল্টি-ফ্যাক্টর অথেনটিকেশন (MFA) এবং নিরাপদ তথ্য ব্যবহার নিশ্চিত করা।

৩. সন্দেহজনক ই-মেইল, ফিশিং, ম্যালওয়্যার অথবা অন্য কোনো নিরাপত্তা ঘটনা তাৎক্ষণিকভাবে রিপোর্ট করা।

৪. সংবেদনশীল তথ্যের গোপনীয়তা বজায় রাখা এবং অনুমোদন ছাড়া তথ্য প্রকাশ না করা।

৫. প্রতিষ্ঠানের তথ্য ও আইসিটি সম্পদের গ্রহণযোগ্য ব্যবহার (Acceptable Use) নিশ্চিত করা।

৬. বাধ্যতামূলক তথ্য নিরাপত্তা সচেতনতা ও প্রশিক্ষণে অংশগ্রহণ করা।

৭. দায়িত্ব পরিবর্তন, বদলি অথবা চাকরি সমাপ্তির সময় প্রতিষ্ঠানের সকল তথ্য ও সম্পদ যথাযথভাবে হস্তান্তর করা।

## ২.৩ নিরাপত্তা শাসন কাঠামো (Security Governance Framework)

ভূমি মন্ত্রণালয় তথ্য নিরাপত্তা ব্যবস্থাপনার কার্যকর তদারকি, জবাবদিহিতা, ঝুঁকি ব্যবস্থাপনা এবং ধারাবাহিক উন্নয়ন নিশ্চিত করার লক্ষ্যে একটি সমন্বিত নিরাপত্তা শাসন কাঠামো (Security Governance Framework) প্রতিষ্ঠা করবে। এ কাঠামো দায়িত্বের স্তরভিত্তিক (Layered Governance Model) নীতির ভিত্তিতে পরিচালিত হবে, যাতে নীতিনির্ধারণ, নিরাপত্তা ব্যবস্থাপনা, কারিগরি বাস্তবায়ন এবং স্বাধীন মূল্যায়নের মধ্যে দায়িত্বের পৃথকীকরণ (Segregation of Duties), জবাবদিহিতা (Accountability) এবং কার্যকর তদারকি (Oversight) নিশ্চিত হয়। এ নিরাপত্তা শাসন কাঠামোতে নিম্নোক্ত উপাদানসমূহ অন্তর্ভুক্ত থাকবে

### ২.৩.১. শাসন কাঠামো (Governance Structure)

১. নীতিনির্ধারণ ও তদারকি স্তর (Governance Layer): Information Security Governance Committee তথ্য নিরাপত্তা নির্দেশনা, মানদণ্ড ও নিরাপত্তা নিয়ন্ত্রণ অনুমোদন, কৌশলগত দিকনির্দেশনা প্রদান, ঝুঁকি গ্রহণযোগ্যতা (Risk Appetite) নির্ধারণ, নিরাপত্তা কর্মসম্পাদন পর্যালোচনা এবং প্রয়োজনীয় নীতিগত সিদ্ধান্ত গ্রহণ করবে।

২. নিরাপত্তা ব্যবস্থাপনা স্তর (Management Layer): CISO/ISO তথ্য নিরাপত্তা নীতি বাস্তবায়ন, ঝুঁকি ব্যবস্থাপনা, কমপ্লায়েন্স, নিরাপত্তা সচেতনতা, ইনসিডেন্ট ব্যবস্থাপনা এবং নিরাপত্তা কার্যক্রমের সমন্বয় ও তদারকি করবে।

৩. কারিগরি বাস্তবায়ন স্তর (Operational Layer): আইটি অপারেশনস ও সিকিউরিটি টিম, সিস্টেমের মালিক (System Owner) এবং তথ্য সম্পদের সংরক্ষক (Information Asset Custodian) অনুমোদিত নিরাপত্তা নিয়ন্ত্রণসমূহ বাস্তবায়ন, নিরাপত্তা পর্যবেক্ষণ, লগ ব্যবস্থাপনা, ভ্যালনারেবিলিটি মূল্যায়ন, প্যাচ ব্যবস্থাপনা, ইনসিডেন্ট প্রতিক্রিয়া এবং ব্যবসায়িক ধারাবাহিকতা (Business Continuity) ও দুর্যোগ পুনরুদ্ধার (Disaster Recovery) কার্যক্রম পরিচালনা করবে।

৪. স্বাধীন মূল্যায়ন স্তর (Assurance Layer): অভ্যন্তরীণ নিরীক্ষা (Internal Audit) এবং প্রয়োজনে স্বাধীন নিরাপত্তা মূল্যায়ন বা বাহ্যিক নিরীক্ষার মাধ্যমে তথ্য নিরাপত্তা নিয়ন্ত্রণ, আইন ও নীতিমালার প্রতিপালন এবং নিরাপত্তা ব্যবস্থাপনার কার্যকারিতা মূল্যায়ন করা হবে।

### ২.৩.২. শাসন নীতি (Governance Principles)

১. তথ্য নিরাপত্তা সংক্রান্ত নীতি প্রণয়ন, নিয়ন্ত্রণ বাস্তবায়ন এবং স্বাধীন মূল্যায়নের দায়িত্ব একই ব্যক্তি বা ইউনিটের উপর অর্পণ করা যাবে না। প্রয়োজনে বিকল্প কর্মকর্তা, পৃথক ইউনিট অথবা পৃথক কমিটির মাধ্যমে দায়িত্বের পৃথকীকরণ (Segregation of Duties) নিশ্চিত করতে হবে।

২. উল্লিখিত নিরাপত্তা শাসন কাঠামোর কার্যকারিতা কমপক্ষে বছরে একবার অথবা গুরুত্বপূর্ণ সাংগঠনিক, প্রযুক্তিগত বা আইনগত পরিবর্তনের ক্ষেত্রে পর্যালোচনা ও প্রয়োজন অনুযায়ী হালনাগাদ করতে হবে।

### ২.৩.৩. নিরাপত্তা ব্যবস্থাপনা কার্যক্রম (Security Management Activities)

১. নীতি ও নিয়ন্ত্রণ কাঠামো (Policies and Control Framework): তথ্য নিরাপত্তা নিয়ন্ত্রণসমূহ ISO/IEC ২৭০০১:২০২২, NIST Cybersecurity Framework, ISACA ITAF, OWASP এবং প্রযোজ্য জাতীয় আইন, বিধি ও নীতিমালার সঙ্গে সামঞ্জস্য রেখে বাস্তবায়ন ও নিয়মিত হালনাগাদ করতে হবে।

২. ঝুঁকি ব্যবস্থাপনা (Risk Management): আইসিটি অবকাঠামো, তথ্য-উপাত্ত, ক্লাউড পরিবেশ এবং তৃতীয় পক্ষের সেবাসহ সকল গুরুত্বপূর্ণ সম্পদের ঝুঁকি নিয়মিতভাবে শনাক্ত, মূল্যায়ন, গ্রহণ (Accept), হ্রাস (Reduce), স্থানান্তর (Transfer) অথবা পরিহার (Avoid) করার জন্য উপযুক্ত ব্যবস্থা গ্রহণ, বাস্তবায়ন এবং নিয়মিত পর্যবেক্ষণ করতে হবে।

৩. ধারাবাহিক পর্যবেক্ষণ ও উন্নয়ন (Continuous Monitoring and Improvement): নিরাপত্তা নিয়ন্ত্রণের কার্যকারিতা, নিরাপত্তা লগ, SIEM সতর্কবার্তা, ভ্যালনারেবিলিটি, নিরাপত্তা ঘটনার প্রবণতা এবং সংশোধনমূলক কার্যক্রম নিয়মিত পর্যবেক্ষণ ও পর্যালোচনা করতে হবে।

৪. রিপোর্টিং ও নিরাপত্তা মেট্রিক্স (Reporting and Security Metrics): নিরাপত্তা পরিস্থিতি, গুরুত্বপূর্ণ ঝুঁকি সূচক (Key Risk Indicators-KRIs), নিরাপত্তা ঘটনার পরিসংখ্যান, কমপ্লায়েন্সের অবস্থা এবং সংশোধনমূলক কার্যক্রমের অগ্রগতি নিয়মিতভাবে (কমপক্ষে ত্রৈমাসিক বা প্রয়োজন অনুযায়ী) সিনিয়র ম্যানেজমেন্টের নিকট উপস্থাপন করতে হবে।

৫. আইসিটি গভর্ন্যান্সের সঙ্গে সমন্বয় (Integration with ICT Governance): সিস্টেম পরিকল্পনা, উন্নয়ন, ক্রয়, বাস্তবায়ন, পরিচালনা, পরিবর্তন ব্যবস্থাপনা (Change Management) এবং সেবা অবসানের প্রতিটি পর্যায়ে তথ্য নিরাপত্তা বিষয়ক প্রয়োজনীয়তা অন্তর্ভুক্ত করতে হবে। "Security by Design" এবং "Security by Default" নীতি অনুসরণ নিশ্চিত করতে হবে এবং সকল নতুন বা পরিবর্তিত তথ্যপ্রযুক্তি সেবায় নিরাপত্তা চাহিদা নকশা পর্যায় থেকেই অন্তর্ভুক্ত করতে হবে।

৬. নিরাপত্তা ব্যতিক্রম ব্যবস্থাপনা (Security Exception Management): কোনো প্রযুক্তিগত, পরিচালনাগত বা ব্যবসায়িক কারণে এই নির্দেশিকার কোনো নিরাপত্তা নিয়ন্ত্রণ সাময়িকভাবে অনুসরণ করা সম্ভব না হলে, সংশ্লিষ্ট ঝুঁকি মূল্যায়ন করে যথাযথ কর্তৃপক্ষের অনুমোদনের ভিত্তিতে ব্যতিক্রম অনুমোদন প্রদান করতে হবে। সকল ব্যতিক্রম নির্ধারিত সময়সীমাসহ নথিভুক্ত ও নিয়মিত পর্যালোচনা করতে হবে।

## ২.৪ আইনগত ও কমপ্লায়েন্স চাহিদা (Compliance and Legal Requirements)

মন্ত্রণালয়কে জাতীয় আইন, বিধি এবং আন্তর্জাতিক মানদণ্ড অনুযায়ী তথ্য নিরাপত্তা ও ডেটা সুরক্ষায় বাধ্য থাকতে হবে। এর মধ্যে রয়েছে-

১. জাতীয় আইন: জাতীয় উপাত্ত ব্যবস্থাপনা আইন, ২০২৬, ব্যক্তিগত উপাত্ত সুরক্ষা আইন, ২০২৬, সাইবার সুরক্ষা আইন, ২০২৬, তথ্য ও যোগাযোগ প্রযুক্তি আইন, ২০০৬ [সংশোধন ২০০৯, সংশোধন ২০১৩], গুরুত্বপূর্ণ তথ্য পরিকাঠামোর ডিজিটাল নিরাপত্তা সুরক্ষা গাইডলাইন ২০২২ এবং সময়ে সময়ে প্রকাশিত সংশ্লিষ্ট সরকারি নির্দেশনা।
২. আন্তর্জাতিক মান: ISO/IEC ২৭০০১:২০২২ (ISMS), OWASP (ওয়েব অ্যাপ্লিকেশন সিকিউরিটি), NIST Cybersecurity Framework (ঝুঁকি ব্যবস্থাপনা ও রেজিলিয়েন্স)।
৩. ডেটা প্রাইভেসি: ব্যক্তিগত ও সংবেদনশীল তথ্য সঠিকভাবে পরিচালনা নিশ্চিত করা।
৪. তৃতীয় পক্ষের চুক্তি: ডেভেলপার / পরামর্শক / ভেন্ডর / সেবা প্রদানকারি / ঠিকাদার প্রতিষ্ঠানের সঙ্গে সব চুক্তিতে নিরাপত্তা, গোপনীয়তা ও আইন/নিয়ম মেনে চলার শর্তাবলী অন্তর্ভুক্ত রাখা।
৫. অডিট ও পর্যালোচনা: নিয়মিত অভ্যন্তরীণ ও বাহ্যিক অডিট পরিচালনা করে নির্দেশিকা, আইন ও আন্তর্জাতিক মানদণ্ডের অনুসরণ যাচাই করা।

## ৩. সম্পদ ব্যবস্থাপনা (Asset Management)

কার্যকর সম্পদ ব্যবস্থাপনা ভূমি মন্ত্রণালয়ের তথ্য ও প্রযুক্তি অবকাঠামো সুরক্ষার জন্য অত্যন্ত গুরুত্বপূর্ণ। ভৌত (Physical) হোক বা ডিজিটাল সকল ক্ষেত্রেই তথ্য-সম্পদকে তাদের সম্পূর্ণ জীবনচক্র (Lifecycle) জুড়ে অর্থাৎ সংগ্রহ থেকে নিষ্পত্তি পর্যন্ত সুশৃঙ্খলভাবে শনাক্ত, শ্রেণিবিন্যাস ও সুরক্ষিত রাখতে হবে।

### ৩.১ তথ্য সম্পদের শ্রেণিবিন্যাস (Information Asset Classification)

সব তথ্য সম্পদকে তাদের সংবেদনশীলতা, গুরুত্ব এবং ক্ষতির সম্ভাব্য প্রভাব অনুযায়ী শ্রেণিবিন্যাস করতে হবে। এতে উপযুক্ত নিরাপত্তা ব্যবস্থা প্রয়োগ করা সম্ভব হবে।

৩.১.১ শ্রেণিবিন্যাস স্তরসমূহ:

ক. সর্বসাধারণের জন্য উন্মুক্ত (Public): যেসব তথ্য প্রকাশের জন্য অনুমোদিত এবং সাধারণ জনগণের ব্যবহারের জন্য উন্মুক্ত। উদাহরণ: সাধারণ নোটিশ, নাগরিক সেবা নির্দেশিকা, FAQ, প্রকাশিত প্রতিবেদন।

খ. অভ্যন্তরীণ ব্যবহার (Internal Use): যেসব তথ্য শুধুমাত্র ভূমি মন্ত্রণালয় ও এর আওতাধীন দপ্তরের অভ্যন্তরীণ প্রশাসনিক কার্যক্রমে ব্যবহারের জন্য নির্ধারিত এবং জনসাধারণের জন্য প্রকাশযোগ্য নয়। উদাহরণ: অফিস নোট, নোটশিট, অভ্যন্তরীণ প্রতিবেদন, সভার কার্যবিবরণী, প্রশাসনিক যোগাযোগ।

গ. গোপনীয় (Confidential): অনুমোদন ছাড়া প্রকাশ পেলে সরকারি কার্যক্রম বা ব্যক্তি অথবা প্রতিষ্ঠানের উল্লেখযোগ্য ক্ষতি হতে পারে। উদাহরণ: ভূমি মালিকানা ডেটা, চলমান তদন্ত প্রতিবেদন, মামলা-সংক্রান্ত তথ্য, অভ্যন্তরীণ নিরাপত্তা মূল্যায়ন প্রতিবেদন, নাগরিকের সংবেদনশীল ব্যক্তিগত তথ্য ইত্যাদি।

ঘ. অতি সংরক্ষিত (Restricted): সর্বোচ্চ নিরাপত্তা প্রয়োজন এমন তথ্য, যার অননুমোদিত প্রবেশ, প্রকাশ, পরিবর্তন, ধ্বংস বা অপব্যবহার জাতীয় গুরুত্বপূর্ণ তথ্য পরিকাঠামো (Critical Information Infrastructure-CII), ভূমিসেবা, সরকারি কার্যক্রম বা রাষ্ট্রীয় নিরাপত্তার জন্য গুরুতর ঝুঁকি সৃষ্টি করতে পারে। এ ধরনের তথ্য শুধুমাত্র অনুমোদিত ব্যক্তি Need-to-Know, Least Privilege এবং Multi-factor Authentication (যেখানে প্রযোজ্য) পদ্ধতির ভিত্তিতে ব্যবহার করতে পারবেন। উদাহরণ: National Land Database, Production Database Credentials, Root Password, Administrator Credentials, Encryption Keys, Backup Encryption Keys, PKI Certificates, Source Code Repository, Disaster Recovery (DR) Credentials এবং Security Configuration Files।

৩.১.২ ব্যক্তিগত উপাত্ত (Private/Personal Data):

কোনো কর্মকর্তা/কর্মচারী বা নাগরিকের ব্যক্তিগত তথ্য অনুমোদিত ব্যক্তি ব্যতীত অন্য কারও নিকট প্রকাশ করা যাবে না। এ ধরনের তথ্যের সংগ্রহ, প্রক্রিয়াকরণ, সংরক্ষণ, ব্যবহার, আদান-প্রদান ও নিষ্পত্তির ক্ষেত্রে "ব্যক্তিগত উপাত্ত সুরক্ষা আইন, ২০২৬" এবং প্রযোজ্য জাতীয় আইন, বিধি, নীতিমালা ও নির্দেশিকা অনুসরণ করতে হবে। ব্যক্তিগত তথ্যের সংবেদনশীলতা ও ঝুঁকির মাত্রা অনুযায়ী এ নির্দেশিকায় বর্ণিত Public, Internal Use, Confidential অথবা Restricted শ্রেণিবিন্যাস অনুযায়ী পরিচালনা করতে হবে। উদাহরণ: জাতীয় পরিচয়পত্র নম্বর, মোবাইল নম্বর, জন্মতারিখ, ব্যক্তিগত যোগাযোগের তথ্য, মানবসম্পদ (HR) সংক্রান্ত তথ্য, বায়োমেট্রিক তথ্য, আর্থিক তথ্য, স্বাস্থ্যসংক্রান্ত তথ্য ইত্যাদি।

৩.১.৩ তথ্য সম্পদের মালিকরা (Asset owners) তাদের নিজস্ব সম্পদের শ্রেণিবিন্যাসের দায়িত্ব পালন করবেন।

৩.১.৪ শ্রেণিবিন্যাস অনুযায়ী সকল তথ্য অবশ্যই "ডাটা হ্যান্ডলিং ও লেবেলিং" এর ক্রমিকে বর্ণিত সংশ্লিষ্ট সুরক্ষা প্রয়োজনীয়তা অনুযায়ী পরিচালনা করতে হবে।

## ৩.২ সম্পদ তালিকা ও মালিকানা (Asset Inventory and Ownership)

ভূমি মন্ত্রণালয়ের আইসিটি সেল একটি কেন্দ্রীয় সম্পদ তালিকা (Asset Register) রক্ষণাবেক্ষণ করবে, যা নিয়মিত (কমপক্ষে বছরে একবার অথবা প্রয়োজন অনুযায়ী) হালনাগাদ করতে হবে,

৩.২.১ কেন্দ্রীয় সম্পদ তালিকা **(Asset Register)** যাতে অন্তর্ভুক্ত থাকবে-

১. হার্ডওয়্যার: সার্ভার, ওয়ার্কস্টেশন, ল্যাপটপ, মোবাইল, ফায়ারওয়াল, রাউটার

২. সফটওয়্যার: অ্যাপ্লিকেশন, অপারেটিং সিস্টেম, ডেটাবেস, ডেভেলপমেন্ট টুল

৩. তথ্য/ডেটা সম্পদ: নাগরিকের ডেটা, ট্যাক্স রেকর্ড, অ্যাপ্লিকেশন সোর্স কোড, GIS Data, ডিজিটাল মৌজা ম্যাপ, স্ক্যানকৃত দলিল, Metadata

৪. ডকুমেন্টেশন (Documentation): সিস্টেম ডকুমেন্টেশন, নেটওয়ার্ক ডায়াগ্রাম, আর্কিটেকচার ডায়াগ্রাম, Standard Operating Procedure (SOP), কনফিগারেশন ডকুমেন্ট, Disaster Recovery (DR) পরিকল্পনা, ব্যাকআপ ডকুমেন্টেশন ইত্যাদি।

৫. ক্লাউড ও ভার্চুয়াল সম্পদ (Cloud and Virtual Assets): Cloud Subscription, Virtual Machine (VM), Container, Storage, Database as a Service (DBaaS), Kubernetes Cluster, Serverless Services ইত্যাদি।

৬. সেবা (Services): Domain, DNS, VPN, API, PKI Certificate, SSL/TLS Certificate, Email Gateway, Identity Management Service ইত্যাদি।

৭. তৃতীয় পক্ষের সম্পদ (Third-party Assets): তৃতীয় পক্ষ বা ক্লাউড সেবা প্রদানকারীর অবকাঠামোতে হোস্টকৃত বা পরিচালিত সিস্টেম, ডেটা, সফটওয়্যার, API, SaaS/PaaS/IaaS সেবা এবং অন্যান্য আইসিটি সম্পদ।

৩.২.২ প্রত্যেক সম্পদের নির্ধারিত মালিক/কাস্টডিয়ান **(Ownership)** থাকবে, যাঁরা নিশ্চিত করবেন-

১. সম্পদের জন্য প্রযোজ্য নিরাপত্তা নিয়ন্ত্রণসমূহ যথাযথভাবে বাস্তবায়িত ও কার্যকর রয়েছে তা নিশ্চিত করা;

২. গ্রহণযোগ্য ব্যবহারের নিয়ম, প্রবেশাধিকার (Access Rights) এবং বিশেষাধিকারপ্রাপ্ত প্রবেশাধিকার (Privileged Access) নির্ধারণ করা;

৩. সম্পদের শ্রেণিবিন্যাস (Classification), ঝুঁকি (Risk) এবং নিরাপত্তা চাহিদা নিয়মিত (কমপক্ষে বছরে একবার অথবা প্রয়োজন অনুযায়ী) পর্যালোচনা করা;

৪. সম্পদের জীবনচক্র (Lifecycle) জুড়ে নিরাপত্তা ও কমপ্লায়েন্স নিশ্চিত করা;

৫. সম্পদ (Asset) অডিট ও হালনাগাদ কার্যক্রম সমন্বয় করা;

৩.২.৩ সম্পদ তালিকায় কমপক্ষে সম্পদের নাম, ইউনিক আইডি, সম্পদের ধরন, অবস্থান, মালিক (Owner), কাস্টডিয়ান (Custodian), শ্রেণিবিন্যাস (Classification), দায়িত্বপ্রাপ্ত ব্যবহারকারী, বর্তমান অবস্থা (Status) এবং জীবনচক্রের (Lifecycle) তথ্য সংরক্ষণ করতে হবে।

## ৩.৩ ডেটা হ্যান্ডলিং ও লেবেলিং (Data Handling and Labelling)

৩.৩.১ সংবেদনশীল ডেটা যথাযথভাবে সুরক্ষিত রাখতে শ্রেণিবিন্যাস অনুযায়ী লেবেলিং ও হ্যান্ডলিং করতে হবে।

১. ডিজিটাল ফাইল, ইমেইল, ডকুমেন্ট ও স্টোরেজ ডিভাইসে শ্রেণিবিন্যাস লেবেল (যেমন: “Confidential”, “Internal Use”) ব্যবহার করতে হবে।
২. ডেটায় প্রবেশাধিকার শুধুমাত্র অনুমোদিত কর্মীদের জন্য সীমাবদ্ধ রাখতে হবে এবং তা অবশ্যই কর্ম-সম্পাদনের প্রয়োজনের ভিত্তিতে প্রদান করতে হবে;
৩. Restricted ও Confidential তথ্য অনুমোদন ছাড়া ব্যক্তিগত ই-মেইল, ব্যক্তিগত ক্লাউড স্টোরেজ বা মেসেজিং প্ল্যাটফর্মে সংরক্ষণ বা প্রেরণ করা যাবে না;
৪. ইলেকট্রনিকভাবে প্রেরিত সংবেদনশীল ডেটা অবশ্যই অনুমোদিত এনক্রিপশন পদ্ধতি ব্যবহার করে এনক্রিপ্ট করতে হবে;
৫. শ্রেণিবিন্যাসকৃত (Classified) ডেটা প্রিন্ট, কপি, ডাউনলোড অথবা বাহ্যিকভাবে শেয়ার করার ক্ষেত্রে নিয়ন্ত্রণ ও লগ সংরক্ষণ করতে হবে।
৬. ভৌত বা ডিজিটাল যেকোনো মাধ্যম ধ্বংস বা বাতিল করার সময় অবশ্যই নিরাপদ নিষ্পত্তি পদ্ধতি (যেমন: data wiping করা বা ডিজিটাল ডিভাইস থেকে ডেটা মুছে ফেলা, shredding করা বা কাগজ বা মিডিয়া টুকরো টুকরো করে কেটে ফেলা যেন ডেটা পুনরুদ্ধার করা না যায়) অনুসরণ করতে হবে।

৩.৩.২ অপসারণযোগ্য মিডিয়া ব্যবস্থাপনা (Removable Media Management)

অপসারণযোগ্য মিডিয়া (যেমন: USB Flash Drive, External Hard Disk/SSD, Memory Card, Optical Media ইত্যাদি) ব্যবহারের ক্ষেত্রে তথ্যের গোপনীয়তা, অখণ্ডতা এবং নিরাপত্তা নিশ্চিত করার লক্ষ্যে নিম্নোক্ত নির্দেশনা অনুসরণ করতে হবে-

১. অনুমোদিত ব্যবহার: অপসারণযোগ্য মিডিয়া শুধুমাত্র প্রয়োজনীয় ও অনুমোদিত সরকারি কাজে ব্যবহার করা যাবে। ব্যবহারের পূর্বে সংশ্লিষ্ট কর্তৃপক্ষ অথবা আইসিটি সেলের অনুমোদন গ্রহণ করতে হবে।

২. এনক্রিপশন (Encryption): Confidential, Restricted বা ব্যক্তিগত (Personal) শ্রেণিবিন্যাসের তথ্য অপসারণযোগ্য মিডিয়ায় সংরক্ষণ বা স্থানান্তরের ক্ষেত্রে অনুমোদিত এনক্রিপশন (Encryption) ব্যবহার করতে হবে।

৩. লগ সংরক্ষণ (Logging): অপসারণযোগ্য মিডিয়ার মাধ্যমে সংবেদনশীল তথ্যের সংরক্ষণ, স্থানান্তর বা কপি করার ক্ষেত্রে প্রয়োজনীয় লগ সংরক্ষণ এবং প্রয়োজনে নিরীক্ষার (Audit) জন্য তা সংরক্ষিত রাখতে হবে।

৪. ম্যালওয়্যার পরীক্ষা (Malware Scanning): মন্ত্রণালয়ের কোনো সিস্টেমে সংযুক্ত করার পূর্বে সকল অপসারণযোগ্য মিডিয়া অনুমোদিত অ্যান্টি-ম্যালওয়্যার বা এন্ডপয়েন্ট সিকিউরিটি সফটওয়্যার দ্বারা স্ক্যান করতে হবে। সংক্রমিত বা সন্দেহজনক কোনো মিডিয়া ব্যবহার করা যাবে না।

## ৩.৪ সম্পদের গ্রহণযোগ্য ব্যবহার (Acceptable Use of Assets)

সকল কর্মকর্তা, কর্মচারী এবং ভেন্ডারগণকে মন্ত্রণালয়ের মালিকানাধীন আইসিটি সম্পদ দায়িত্বশীলভাবে এবং শুধুমাত্র অনুমোদিত কাজে ব্যবহার করতে হবে। গ্রহণযোগ্য ব্যবহারের নির্দেশনাসমূহ-

১. অফিসিয়াল সিস্টেম কোনো অবস্থাতেই অকার্যকর বা ব্যক্তিগত কাজে ব্যবহার করা যাবে না;
২. মন্ত্রণালয়ের মালিকানাধীন ডিভাইসে অননুমোদিত সফটওয়্যার বা টুল ইনস্টল করা সম্পূর্ণরূপে নিষিদ্ধ;
৩. অনুমোদন ছাড়া ব্যক্তিগত (Bring Your Own Device- BYOD) যেমন: ব্যক্তিগত মোবাইল ফোন, ল্যাপটপ, ট্যাবলেট বা কম্পিউটার ডিভাইস ব্যবহার করে মন্ত্রণালয়ের তথ্য বা সিস্টেমে প্রবেশ করা যাবে না;
৪. ইন্টারনেট ব্যবহার দায়িত্বশীলভাবে করতে হবে, নিষিদ্ধ ওয়েবসাইট ও কনটেন্ট পরিহার করতে হবে;
৫. অপসারণযোগ্য মিডিয়া (যেমন: USB Flash Drive, External Storage, Memory Card ইত্যাদি) শুধুমাত্র এ নির্দেশিকার ৩.৩.১ উপ-অনুচ্ছেদ বর্ণিত শর্ত ও অনুমোদন অনুযায়ী ব্যবহার করা যাবে।
৬. কোনো ধরণের অপব্যবহার বা সন্দেহজনক কার্যকলাপ দেখা গেলে তা অবিলম্বে আইসিটি সিকিউরিটি টিমকে জানাতে হবে।
৭. প্রত্যেক ব্যবহারকারীর নিকট থেকে Acceptable Use Agreement-এ স্বাক্ষর গ্রহণ করতে হবে।

## ৩.৫ সম্পদের জীবনচক্র ব্যবস্থাপনা (Asset Lifecycle Management)

মন্ত্রণালয় আইসিটি সম্পদের পুরো লাইফসাইকেল ব্যবস্থাপনা নিশ্চিত করার জন্য আনুষ্ঠানিক প্রক্রিয়া প্রণয়ন করবে, এতে অন্তর্ভুক্ত থাকবে-

১. সংগ্রহ (Procurement): নতুন হার্ডওয়্যার, সফটওয়্যার ও সংশ্লিষ্ট আইসিটি সেবা শুধুমাত্র অনুমোদিত উৎস বা চ্যানেল থেকে সংগ্রহ করতে হবে এবং সংগ্রহের পূর্বে নিরাপত্তা, লাইসেন্স, সমর্থন (Support) ও কমপ্লায়েন্স যাচাই করতে হবে।
২. স্থাপন (Deployment): সম্পদ নিরাপদভাবে কনফিগার করে ইনভেন্টরিতে নিবন্ধন করতে হবে এবং অনুমোদিত ব্যবহারকারীর কাছে হস্তান্তর করতে হবে।
৩. রক্ষণাবেক্ষণ (Maintenance): নিয়মিত সফটওয়্যার আপডেট, সিকিউরিটি প্যাচ ও সার্ভিসিং করতে হবে।
৪. সংরক্ষণ ও ব্যাকআপ (Storage and Backup): সম্পদের তথ্য নিয়মিত ব্যাকআপ, নিরাপদ সংরক্ষণ এবং প্রয়োজন অনুযায়ী পুনরুদ্ধার (Restore) পরীক্ষার ব্যবস্থা নিশ্চিত করতে হবে।
৫. হস্তান্তর (Transfer): ব্যবহারকারী বা দপ্তরের মধ্যে সম্পদ হস্তান্তরের রেকর্ড রাখতে হবে।
৬. নিষ্পত্তি (Disposal): যেসব সম্পদের কার্যকাল শেষ (End-of-life) বা মেয়াদোত্তীর্ণ হয়ে গেছে, সেসব সম্পদ অবশ্যই নিরাপদভাবে ধ্বংস, বাতিল বা নিষ্পন্ন করতে হবে। এতে সংরক্ষিত সকল তথ্য অনুমোদিত Secure Erase, Cryptographic Erase অথবা Physical Destruction পদ্ধতি অনুসরণ করে স্থায়ীভাবে মুছে ফেলতে (Data Wipe) বা ধ্বংস করতে হবে যেন ডেটা পুনরুদ্ধার (Recovery) করা সম্ভব না হয় এবং ডেটা ধ্বংসের প্রমাণ সংরক্ষণ করতে হবে।
    - নিষ্পত্তি সংক্রান্ত লগ অডিট প্রমাণ হিসেবে নিরীক্ষার জন্য সংরক্ষণ করতে হবে।

৭. End-of-Support (EOS) বা End-of-Life (EOL) অবস্থায় থাকা হার্ডওয়্যার, সফটওয়্যার বা অপারেটিং সিস্টেম ঝুঁকি মূল্যায়ন ব্যতীত ব্যবহার করা যাবে না এবং প্রয়োজন অনুযায়ী তা প্রতিস্থাপন বা আপগ্রেড করতে হবে।

৮. অডিট (Audit): সম্পদের তথ্য ও ব্যবহার সম্পর্কিত সঠিকতা যাচাইয়ের জন্য কমপক্ষে বছরে একবার অথবা ঝুঁকিভিত্তিক (Risk-based) প্রয়োজন অনুযায়ী Physical ও Logical ইনভেন্টরি অডিট পরিচালনা করতে হবে এবং এছাড়াও প্রয়োজনে নমুনাভিত্তিক যাচাই (Sample Verification) পরিচালনা করতে হবে।

## ৪. তথ্য নিরাপত্তা ঝুঁকি ব্যবস্থাপনা (Information Security Risk Management)

তথ্য নিরাপত্তা ঝুঁকি ব্যবস্থাপনার জন্য একটি কাঠামোবদ্ধ ও সক্রিয় পদ্ধতি ভূমি মন্ত্রণালয়ের সম্পদ, সেবা এবং নাগরিকদের ডেটাকে পরিবর্তনশীল হুমকি থেকে সুরক্ষিত রাখতে অপরিহার্য। মন্ত্রণালয় তথ্য সিস্টেমের ঝুঁকি শনাক্ত, মূল্যায়ন, নিয়ন্ত্রণ ও পর্যবেক্ষণ করবে যা ISO/IEC ২৭০০১:২০২২ এবং NIST CSF এর সঙ্গে সামঞ্জস্যপূর্ণ।

### ৪.১ ঝুঁকি ব্যবস্থাপনা কাঠামো (Risk Management Framework - RMF)

মন্ত্রণালয় একটি সমন্বিত ঝুঁকি ব্যবস্থাপনা কাঠামো গ্রহণ করবে, যাতে ঝুঁকি ব্যবস্থাপনা হয় নিয়মিত, স্বচ্ছ ও পুনরাবৃত্তিযোগ্য, এতে থাকবে-

১. ঝুঁকি সনাক্তকরণ (Risk Identification): তথ্য সম্পদের ওপর প্রভাব ফেলতে পারে এমন সম্ভাব্য হুমকি, দুর্বলতা এবং প্রভাব চিহ্নিত করা।

২. ঝুঁকি বিশ্লেষণ (Risk Analysis): সংজ্ঞায়িত ঝুঁকি ম্যাট্রিক্স ব্যবহার করে সম্ভাব্যতা এবং প্রভাব মূল্যায়ন (গুণগত মান qualitatively বা পরিমাণগতভাবে quantitatively) করা।

৩. ঝুঁকি মূল্যায়ন (Risk Evaluation): মূল্যায়িত ঝুঁকিগুলো মন্ত্রণালয়ের ঝুঁকি গ্রহণ ক্ষমতা (risk appetite) এবং সহনশীলতা (tolerance) স্তরের সাথে তুলনা করা।

৪. ঝুঁকি ব্যবস্থাপনা (Risk Treatment): উপযুক্ত ঝুঁকি হ্রাস পদক্ষেপ নির্বাচন বা বাছাইপূর্বক গ্রহণ (Accept), এড়ানো (Avoid), স্থানান্তর (Transfer) বা হ্রাস (Reduce) করা।

৫. ঝুঁকি যোগাযোগ (Risk Communication): ঝুঁকি এবং ঝুঁকি হ্রাসের অবস্থা সংশ্লিষ্ট স্টেকহোল্ডারদের অবহিত করা।

৬. ঝুঁকি পর্যবেক্ষণ (Risk Monitoring): সনাক্ত ঝুঁকির ধারাবাহিক পর্যবেক্ষণ এবং নতুন ঝুঁকি উদ্ভব সনাক্ত করা।

#### ৪.১.১ ঝুঁকি মূল্যায়নের মানদণ্ড (Risk Criteria)

মন্ত্রণালয় ঝুঁকি মূল্যায়নের পূর্বে Risk Criteria নির্ধারণ করবে, যার মধ্যে অন্তর্ভুক্ত থাকবে-

১. গ্রহণযোগ্য ঝুঁকির মাত্রা (Acceptable Risk Level)

২. ঝুঁকি গ্রহণ ক্ষমতা (Risk Appetite)

৩. ঝুঁকি সহনশীলতা (Risk Tolerance)

৪. আইনগত ও নিয়ন্ত্রক বাধ্যবাধকতা

৫. সেবার গুরুত্ব (Business Criticality)

৬. CIA (Confidentiality, Integrity, Availability)-এর উপর সম্ভাব্য প্রভাব

ঝুঁকি ব্যবস্থাপনা কাঠামো (RMF) নথিভুক্ত করতে হবে এবং কমপক্ষে প্রতি বছর বা উল্লেখযোগ্য সিস্টেম পরিবর্তন বা হুমকি পরিবর্তনের পর পর্যালোচনা করতে হবে।

## ৪.২ ঝুঁকি মূল্যায়ন ও মোকাবিলা (Risk Assessment and Treatment)

মন্ত্রণালয় তার আইসিটি পরিবেশে প্রভাব ফেলার সম্ভাব্য সাইবার নিরাপত্তা ঝুঁকিগুলো মূল্যায়নের জন্য আনুষ্ঠানিক ঝুঁকি মূল্যায়ন (Risk Assessment) পরিচালনা করবে, যার মধ্যে অন্তর্ভুক্ত থাকবে:

১. ওয়েব অ্যাপ্লিকেশন ও প্ল্যাটফর্ম (যেমন: e-Porcha, LMS, LDTAX)
২. অভ্যন্তরীণ আইটি অবকাঠামো (সার্ভার, ডেটাবেস, এন্ডপয়েন্ট, নেটওয়ার্ক)
৩. ক্লাউড ও তৃতীয় পক্ষের হোস্টেড সেবা
৪. ডেটা শ্রেণিবিন্যাস এবং প্রাইভেসি প্রভাব মূল্যায়ন

প্রতিটি ঝুঁকি মূল্যায়নের ক্ষেত্রে নিম্নলিখিত শর্তাবলী প্রযোজ্য হবে:

১. তথ্য নিরাপত্তা কর্মকর্তা (ISO) নেতৃত্ব দেবেন এবং সিস্টেম মালিক ও আইটি টিম সহযোগিতা করবে।
২. একটি মানসম্মত টেমপ্লেট এবং স্কোরিং মডেল (যেমন: High/Medium/Low) ব্যবহার করবে।
৩. প্রযুক্তিগত ঝুঁকি (যেমন: প্যাচ না হওয়া সিস্টেম, কোড দুর্বলতা) এবং সাংগঠনিক ঝুঁকি (যেমন: নীতির অভাব, অ্যাক্সেস কন্ট্রোল দুর্বলতা) উভয়ই অন্তর্ভুক্ত থাকবে।
৪. সমাধানের জন্য সুনির্দিষ্ট ঝুঁকি হ্রাস পরিকল্পনা, দায়িত্বশীল ব্যক্তি এবং সময়সীমা নির্ধারণ করতে হবে।
৫. ঝুঁকি মূল্যায়ন কমপক্ষে বার্ষিকভাবে, অথবা সিস্টেম স্থাপনের আগে, বড় আপগ্রেড বা পরিবর্তনের আগে পরিচালনা করতে হবে।

সমস্ত ঝুঁকি হ্রাস সম্পর্কিত সিদ্ধান্ত ম্যানেজমেন্ট কর্তৃক অনুমোদিত হতে হবে এবং ঝুঁকি রেজিস্টারে (Risk Register) নথিভুক্ত করতে হবে।

## ৪.৩ ঝুঁকি নিবন্ধন ও ট্র্যাকিং (Risk Register and Mitigation Tracking)

মন্ত্রণালয়ের সমস্ত সনাক্ত ঝুঁকির লগ এবং পর্যবেক্ষণের জন্য একটি কেন্দ্রীভূত ঝুঁকি রেজিস্টার (Risk Register) রক্ষণাবেক্ষণ করতে হবে। এই রেজিস্টারে অন্তর্ভুক্ত থাকবে-

১. স্বতন্ত্র ঝুঁকি শনাক্তকরণ নম্বর (Unique Risk Identifier);
২. ঝুঁকির শিরোনাম ও বিবরণ (Risk Title and Description);
৩. ঝুঁকির ধরন বা শ্রেণি (Risk Category) (যেমন: প্রযুক্তিগত, পরিচালনাগত, মানবসম্পদ, আইনগত, তৃতীয় পক্ষ, ক্লাউড, সাইবার নিরাপত্তা ইত্যাদি);
৪. প্রভাবিত সম্পদ, সিস্টেম বা সেবা (Affected Asset/System/Service);
৫. সম্ভাব্য হুমকি (Threat), দুর্বলতা (Vulnerability), সম্ভাব্যতা (Likelihood) এবং প্রভাব (Impact);
৬. প্রাথমিক ঝুঁকি রেটিং (Inherent Risk Rating);
৭. বিদ্যমান নিরাপত্তা নিয়ন্ত্রণসমূহ (Existing Security Controls);
৮. ঝুঁকির মালিক (Risk Owner);
৯. নির্বাচিত ঝুঁকি মোকাবিলা পদ্ধতি (Risk Treatment Option) - গ্রহণ (Accept), পরিহার (Avoid), হ্রাস (Reduce) অথবা স্থানান্তর (Transfer);
১০. ঝুঁকি হ্রাস কার্যপরিকল্পনা (Risk Treatment Plan), দায়িত্বপ্রাপ্ত ব্যক্তি এবং লক্ষ্যসমাপ্তির তারিখ (Target Remediation Date);

১১. বর্তমান বাস্তবায়ন বা সমাধানের অবস্থা (Current Mitigation Status);
১২. অবশিষ্ট ঝুঁকি রেটিং (Residual Risk Rating);
১৩. পরবর্তী পর্যালোচনার তারিখ (Next Review Date); এবং
১৪. ঝুঁকির বর্তমান অবস্থা (Risk Status) (যেমন: Open, In Progress, Accepted, Closed)।

ঝুঁকি রেজিস্টারটি প্রতি ত্রৈমাসিকে (Quarterly) Information Security Governance Committee দ্বারা পর্যালোচনা করতে হবে, যেন ঝুঁকিগুলো সময়মতো সমাধান হচ্ছে কিনা নিশ্চিত করা যায় এবং যেকোনো বিলম্বিত বা গুরুত্বপূর্ণ ঝুঁকি উর্দ্ধতন কর্তৃপক্ষের নিকট দ্রুত প্রেরণ করা যায়।

## ৪.৪ তৃতীয় পক্ষের ঝুঁকি ব্যবস্থাপনা (Third-Party Risk Management)

মন্ত্রণালয়ের তথ্য-উপাত্ত, সিস্টেম ও সেবার নিরাপত্তা নিশ্চিত করার লক্ষ্যে তৃতীয় পক্ষ (যেমন: ভেন্ডর, সেবা প্রদানকারী, ক্লাউড সেবা প্রদানকারী, পরামর্শক ও আউটসোর্সিং প্রতিষ্ঠান) সম্পর্কিত ঝুঁকি যথাযথভাবে শনাক্ত, মূল্যায়ন, নিয়ন্ত্রণ এবং পর্যবেক্ষণ করতে হবে। নিম্নলিখিত নিয়ন্ত্রণসমূহ বাস্তবায়ন করতে হবে-

১. সব ভেন্ডরের নিরাপত্তা পূর্বপরীক্ষা (Security Due Diligence) করা হবে, যার মধ্যে তাদের অবকাঠামো, প্রক্রিয়া এবং সার্টিফিকেশন মূল্যায়ন অন্তর্ভুক্ত থাকবে।
২. মন্ত্রণালয়ের তথ্য বা সিস্টেমে তৃতীয় পক্ষের প্রবেশাধিকার সর্বনিম্ন প্রয়োজনীয়তার (Least Privilege) ভিত্তিতে, নির্দিষ্ট সময়ের জন্য, অনুমোদনসাপেক্ষে প্রদান করতে হবে এবং সকল প্রবেশাধিকার নিয়মিত পর্যবেক্ষণ, পর্যালোচনা ও প্রয়োজন শেষ হলে বাতিল করতে হবে।
৩. সব চুক্তি (Contract), সমঝোতা স্মারক (MoU), Service Level Agreement (SLA) অথবা Non-Disclosure Agreement (NDA)-এ তথ্য নিরাপত্তা, ব্যক্তিগত উপাত্ত সুরক্ষা, গোপনীয়তা, নিরাপত্তা ঘটনা (Incident) রিপোর্টিং, নিরীক্ষার অধিকার (Right to Audit), আইনগত দায়বদ্ধতা, সেবা সমাপ্তির (Exit) পর ডেটা ফেরত বা নিরাপদ ধ্বংস এবং প্রযোজ্য আইন অনুসরণের শর্ত অন্তর্ভুক্ত থাকতে হবে।
৪. গোপনীয় বা সংবেদনশীল ডেটায় এক্সেসপ্রাপ্ত ভেন্ডর প্রাসঙ্গিক মানদণ্ডের (যেমন ISO ২৭০০১, SOC ২ ইত্যাদি) সঙ্গে সম্মতি প্রদর্শনের প্রমাণ অথবা সমমানের স্বাধীন নিরাপত্তা মূল্যায়ন প্রতিবেদন প্রদান করতে হবে।
৫. পর্যায়ক্রমিক ভেন্ডর ঝুঁকি মূল্যায়ন (Vendor Risk Assessment) পরিচালনা করতে হবে, যেন তাদের নিরাপত্তা অবস্থার পুনর্মূল্যায়ন করা যায়। এ মূল্যায়ন কমপক্ষে বছরে একবার অথবা চুক্তির নবায়ন, গুরুত্বপূর্ণ পরিবর্তন বা নিরাপত্তা ঘটনার পর পুনরায় পরিচালনা করতে হবে।
৬. ভেন্ডরের সফটওয়্যার, API, লাইব্রেরি, ওপেন সোর্স কম্পোনেন্ট এবং সফটওয়্যার সাপ্লাই চেইনের নিরাপত্তা ঝুঁকি নিয়মিত মূল্যায়ন করতে হবে এবং সফটওয়্যারের উৎস, অখণ্ডতা (Integrity) ও নির্ভরযোগ্যতা নিশ্চিত করতে প্রয়োজনীয় নিরাপত্তা নিয়ন্ত্রণ বাস্তবায়ন করতে হবে।
৭. ভেন্ডর হোস্টেড পরিবেশের ক্ষেত্রে, স্বাধীন পেনিট্রেশন টেস্টিং, ভ্যালনারেবিলিটি মূল্যায়ন (Vulnerability Assessment) এবং প্রয়োজনে সোর্স কোড রিভিউ পরিচালনা করতে হবে এবং ফলাফল মন্ত্রণালয়ের কাছে প্রতিবেদন আকারে প্রদান করতে হবে।
৮. তৃতীয় পক্ষের নিরাপত্তা কর্মসম্পাদন (Security Performance) নিয়মিত পর্যবেক্ষণ করতে হবে এবং চুক্তিভিত্তিক নিরাপত্তা শর্তাবলীর প্রতিপালন (Compliance) পর্যায়ক্রমে পর্যালোচনা করতে হবে।

৯. চুক্তি সমাপ্তি, বাতিল বা সেবা প্রদানকারীর পরিবর্তনের ক্ষেত্রে মন্ত্রণালয়ের তথ্য নিরাপদভাবে ফেরত, স্থানান্তর অথবা ধ্বংস নিশ্চিত করতে হবে এবং তৃতীয় পক্ষের সকল প্রবেশাধিকার অবিলম্বে প্রত্যাহার করতে হবে।

## ৫. সরবরাহকারী নিরাপত্তা ব্যবস্থাপনা (Supplier Security Management)

ভূমি মন্ত্রণালয় অ্যাপ্লিকেশন ডেভেলপমেন্ট, রক্ষণাবেক্ষণ, হোস্টিং এবং অন্যান্য আইসিটি কার্যক্রমের জন্য বহিরাগত ভেন্ডর ও সার্ভিস প্রোভাইডারের ওপর নির্ভর করে। যেহেতু এই সরবরাহকারীরা সংবেদনশীল সিস্টেম ও ডেটায় প্রবেশাধিকার পায়, তাই তাদের পুরো কার্যকালীন সময় জুড়ে নিরাপত্তা ব্যবস্থাপনা করা অত্যন্ত জরুরি। এই অধ্যায়ে সরবরাহকারীদের জন্য নীতি ও নিয়ন্ত্রণ ব্যবস্থা বর্ণনা করা হলো যেন তারা মন্ত্রণালয়ের তথ্য নিরাপত্তা ও ডেটা সুরক্ষার চাহিদা পূরণ করে।

### ৫.১ সরবরাহকারী মূল্যায়ন ও যথাযথ সতর্কতা (Supplier Evaluation and Due Diligence)

কোনো চুক্তি স্বাক্ষরের আগে সকল সরবরাহকারীকে একটি কাঠামোবদ্ধ নিরাপত্তা মূল্যায়ন ও যথাযথ সতর্কতার প্রক্রিয়ার মধ্য দিয়ে যেতে হবে। এতে অন্তর্ভুক্ত থাকবে—

১. সরবরাহকারীর প্রযুক্তিগত সক্ষমতা, সার্টিফিকেশন (যেমন: ISO/IEC ২৭০০১, SOC ২) ও পূর্বের নিরাপত্তা রেকর্ড মূল্যায়ন।
২. তাদের অভ্যন্তরীণ নীতি, কর্ম-সম্পাদন ধারাবাহিকতা পরিকল্পনা ও এক্সেস কন্ট্রোল যাচাই।
৩. সাক্ষাৎকার গ্রহণ এবং প্রয়োজনে সরবরাহকারীর সাইটে (ফিজিক্যাল/ভার্চুয়াল) অডিট।
৪. তারা অন্য সরকারি বা গুরুত্বপূর্ণ অবকাঠামোর ডেটা পরিচালনা করে কিনা তা যাচাই।
৫. ভেন্ডর রিস্ক স্কোরিং মডেল ব্যবহার করে ঝুঁকি মূল্যায়ন ও নিয়ন্ত্রণ নির্ধারণ।
৬. যথাযথ সতর্কতার ফলাফল নথিভুক্ত করতে হবে এবং Information Security Governance Committee দ্বারা অনুমোদিত হতে হবে।

### ৫.২ চুক্তিভিত্তিক নিরাপত্তা শর্ত (Contractual Security Requirements)

মন্ত্রণালয়ের ডেটা বা সিস্টেমে প্রবেশাধিকার থাকা সব সরবরাহকারীর সঙ্গে করা চুক্তিতে স্পষ্ট নিরাপত্তা ও কমপ্লায়েন্স শর্ত থাকতে হবে। যেমন-

১. ডেটা সুরক্ষা ও গোপনীয়তার বাধ্যবাধকতা;
২. কর্তৃপক্ষের অনুমোদন ব্যতিরেকে সাব-কন্ট্রাক্টিং না করার শর্ত;
৩. অডিট পরিচালনার অধিকার এবং সাইটে সরেজমিন পরিদর্শনের বিধান;
৪. ইনসিডেন্ট রিপোর্টিং এর সময়সীমা ও পর্যায়ক্রমিক অবহিতকরণ (Escalation) প্রক্রিয়া;
৫. তথ্য এনক্রিপশন, নিরাপদ আদান-প্রদান ও ডেটা সংরক্ষণের জন্য বাধ্যতামূলক শর্তাবলী;
৬. সরবরাহকারীর সংশ্লিষ্ট সকল কর্মীদের নিকট হতে Non-Disclosure Agreement (NDA) গ্রহণের শর্ত;
৭. গুরুত্বের মাত্রা বিবেচনায় দুর্বলতা/আক্রম্যতা নিরসন ও ইনসিডেন্ট প্রতিক্রিয়ার সময়সীমা অন্তর্ভুক্ত রাখা;
৮. চুক্তির টেমপ্লেট প্রতি বছর পর্যালোচনা করতে হবে যেন তা নতুন আইন ও নিয়মের সঙ্গে সামঞ্জস্যপূর্ণ হয়।

### ৫.৩ তৃতীয় পক্ষের প্রবেশাধিকার নিয়ন্ত্রণ (Third-Party Access Controls)

যেসকল ভেন্ডারদের মন্ত্রণালয়ের পরিবেশে (ডেভেলপমেন্ট, টেস্ট, প্রোডাকশন) প্রবেশাধিকারের প্রয়োজন তাদের কঠোর প্রবেশাধিকার নিয়ন্ত্রণ (Strict Access Control) নীতিমালা মেনে চলতে হবে-

১. প্রবেশাধিকার শুধুমাত্র সুনির্দিষ্ট কাজ ও নির্দিষ্ট সময়ের জন্য প্রদান করা হবে;

২. নিরাপদ চ্যানেলের মাধ্যমে (যেমন: VPN + MFA) সিস্টেমে প্রবেশ নিশ্চিত করতে হবে;

৩. দূর নিয়ন্ত্রণ প্রবেশ (Remote Access) এর লগ নিয়মিতভাবে পর্যবেক্ষণ ও পর্যালোচনা করতে হবে;

৪. প্রতিটি ভেন্ডরের জন্য আলাদা ইউজার অ্যাকাউন্ট ব্যবহার করতে হবে যেখানে শেয়ার্ড ক্রিডেনশিয়াল সম্পূর্ণ নিষিদ্ধ;

৫. ভেন্ডরগণ লাইভ সিস্টেমে পরিবর্তন/পরিবর্ধন/পরিমার্জনের জন্য কর্তৃপক্ষের লিখিত অনুমোদন নিশ্চিত করতে হবে;

৬. কোনো কাজ সম্পন্ন হওয়া বা চুক্তি সমাপ্তির সাথে সাথে ভেন্ডার অ্যাকাউন্ট অবিলম্বে নিষ্ক্রিয় করতে হবে;

### ৫.৪ সরবরাহকারী ঝুঁকি মূল্যায়ন (Supplier Risk Assessment)

সরবরাহকারীদেরকে নিয়মিতভাবে নিরাপত্তা ঝুঁকি মূল্যায়নের মাধ্যমে পর্যালোচনা করতে হবে, যার মধ্যে নিম্নোক্ত বিষয়গুলো অন্তর্ভুক্ত থাকবে:

১. তথ্য-উপাত্ত পরিচালনা ও সংশ্লিষ্ট ঝুঁকির প্রভাব;

২. চুক্তিতে নির্ধারিত শর্ত সঠিকরূপে প্রতিপালিত হচ্ছে কিনা;

৩. সাম্প্রতিক কোনো পরিবর্তন, নিরাপত্তা ইনসিডেন্ট বা অডিট ফলাফল পর্যালোচনা;

৪. নিজস্ব অভ্যন্তরীণ তথ্য নিরাপত্তা ব্যবস্থাপনা সিস্টেম (ISMS) এবং তথ্য সুরক্ষা নিয়ন্ত্রণের পরিপক্কতা;

৫. সাব-প্রসেসর বা হোস্টিং প্ল্যাটফর্মের ওপর নির্ভরতা।

### ৫.৫ সরবরাহকারীর কার্যকারিতা পর্যবেক্ষণ ও পর্যালোচনা (Monitoring and Review of Supplier Performance)

মন্ত্রণালয় চুক্তি কার্যকালীন সময়ে সরবরাহকারীর কার্যকারিতা নিয়মিতভাবে পর্যবেক্ষণ ও পর্যালোচনা করবে যেন নিরাপত্তা সংক্রান্ত প্রত্যাশা নিশ্চিত করা যায় এবং যেখানে নিম্নোক্ত বিষয়াদি অন্তর্ভুক্ত থাকবে-

১. ত্রৈমাসিক পারফরম্যান্স রিভিউ (নিরাপত্তা মেট্রিক্স ও ইনসিডেন্ট রিপোর্টসহ);

২. প্যাচিং স্ট্যাটাস, চেঞ্জ লগ ও নিরাপত্তা পরীক্ষার ফলাফল (যেমন: VAPT রিপোর্ট) যাচাই;

৩. তৃতীয় পক্ষের বর্ষিক অডিট রিপোর্ট, যা সরবরাহকারীরা মন্ত্রণালয়ের চাহিদামত সরবরাহ করবে;

৪. মন্ত্রণালয়ের স্টেকহোল্ডারদের নিকট সার্ভের মাধ্যমে প্রাপ্ত ফিডব্যাক ফলাফল;

৫. গুরুতর বা বারবার নিরাপত্তা ভঙ্গের ক্ষেত্রে সরবরাহকারীর সেবা স্থগিত বা বাতিল করার ক্ষমতা।

## ৬. নিরাপত্তা ব্যবস্থাপনা ও প্রক্রিয়া (Security Management and Procedures)

একটি স্থায়ী এবং নিরাপদ আইসিটি পরিবেশ বজায় রাখার জন্য আনুষ্ঠানিক ও বাধ্যতামূলক নিরাপত্তা ব্যবস্থা প্রণয়ন করা অপরিহার্য। এসকল ব্যবস্থাপনায় ব্যবহারকারী, আইটি কর্মী এবং তৃতীয় পক্ষের স্টেকহোল্ডারদের কাছে তথ্য এবং সিস্টেম কীভাবে সুরক্ষিত রাখতে হবে তা স্পষ্টভাবে নির্দেশ করে। ভূমি মন্ত্রণালয়ের জন্য প্রয়োজনীয় ব্যবস্থাপনা প্রণয়ন, বাস্তবায়ন এবং নিয়মিত পর্যালোচনা করতে হবে যেন নিরাপত্তা ঝুঁকি কমানো যায় এবং নিয়ন্ত্রক চাহিদার সঙ্গে সঙ্গতি বজায় রাখা যায়।

### ৬.১ গ্রহণযোগ্য ব্যবহার নীতি (Acceptable Use Policy)

গ্রহণযোগ্য ব্যবহার নীতি (Acceptable Use Policy) নির্ধারণ করে যে কিভাবে মন্ত্রণালয়-স্বত্ত্বাধিকারভুক্ত সিস্টেম, নেটওয়ার্ক, সফটওয়্যার এবং ডেটা ব্যবহারকারী, ঠিকাদার ও ভেন্ডরদের দ্বারা ব্যবহার করা হবে। প্রধান উপাদানসমূহ হলো-

১. আইসিটি সম্পদ শুধুমাত্র অফিসিয়াল এবং অনুমোদিত উদ্দেশ্যে ব্যবহার করা যাবে;

২. ব্যক্তিগত ব্যবহার সীমিত রাখতে হবে এবং কাজ বা নিরাপত্তায় বাধা সৃষ্টি করা যাবে না;

৩. ব্যবহারকারীরা অনুমোদনবিহীন সফটওয়্যার ইনস্টল করতে, ব্যক্তিগত ডিভাইস সংযুক্ত করতে বা নিষিদ্ধ ওয়েবসাইটে প্রবেশ করতে পারবে না;

৪. মন্ত্রণালয়ের তথ্য কখনোই পাবলিক ফোরাম, ব্যক্তিগত ইমেইল বা অননুমোদিত ক্লাউড প্ল্যাটফর্মে শেয়ার করা যাবে না;

৫. কোনো অপব্যবহার বা নীতি ভঙ্গের সন্দেহ হলে তাৎক্ষণিকভাবে Information Security Officer-কে অবহিত করতে হবে;

৬. প্রত্যেক ব্যবহারকারীর নিকট হতে নিয়োগ বা সিস্টেমে অ্যাক্সেস পাওয়ার সময় গ্রহণযোগ্য ব্যবহার নীতির (AUP) তে স্বীকৃতি স্বাক্ষর গ্রহণ করতে হবে।

### ৬.২ পাসওয়ার্ড ব্যবস্থাপনা (Password Management)

এই ব্যবস্থা শক্তিশালী অথেন্টিকেশন নিশ্চিত করতে এবং অননুমোদিত প্রবেশ ঠেকাতে প্রযোজ্য।

১. পাসওয়ার্ড ন্যূনতম ১২ অক্ষরের হতে হবে এবং তাতে বড়-ছোট হাতের অক্ষর, সংখ্যা ও বিশেষ চিহ্ন থাকতে হবে;

২. প্রতি ৯০ দিনে পাসওয়ার্ড পরিবর্তন করতে হবে;

৩. আগের কমপক্ষে ৩টি পাসওয়ার্ড পুনর্ব্যবহার করা যাবে না;

৪. সিস্টেম বা অ্যাপ্লিকেশনের ডিফল্ট পাসওয়ার্ড ইনস্টলেশনের পরপরই বদলাতে হবে;

৫. সব প্রিভিলেজড অ্যাকাউন্ট, রিমোট ইউজার ও অ্যাডমিনদের জন্য MFA (Multi-Factor Authentication) বাধ্যতামূলক;

৬. পাসওয়ার্ড কখনোই শেয়ার করা যাবে না বা plaintext-এ সংরক্ষণ করা যাবে না;

৭. অনুমোদিত পাসওয়ার্ড ম্যানেজার ব্যবহার করা যাবে ।

## ৬.৩ রিমোট এক্সেস ব্যবস্থাপনা (Remote Access Management)

দূর থেকে কাজ করা বা তৃতীয় পক্ষের সহযোগিতা সুরক্ষিত করতে রিমোট এক্সেসের জন্য কঠোর ব্যবস্থাপনা মেনে চলতে হবে।

১. সব রিমোট এক্সেস এনক্রিপটেড চ্যানেল (VPN + MFA) এর মাধ্যমে করতে হবে।

২. কেবল অনুমোদিত এবং ব্যবসায়িক প্রয়োজনযুক্ত ইউজাররা এক্সেস পাবে।

৩. Remote Desktop Protocols ব্যবহার করলে তা শক্তিশালীভাবে কনফিগার ও মনিটর করতে হবে।

৪. নির্দিষ্ট সময় নিষ্ক্রিয় থাকলে সেশন স্বয়ংক্রিয়ভাবে বন্ধ হয়ে যাবে।

৫. রিমোট সেশনের সময় মন্ত্রণালয়ের ডেটা ব্যক্তিগত ডিভাইসে ডাউনলোড করা যাবে না।

৬. রিমোট এক্সেসের জন্য ব্যবহৃত সব ডিভাইসে এন্ডপয়েন্ট প্রটেকশন ও কমপ্লায়েন্স চেক থাকতে হবে।

৭. রিমোট এক্সেস লগ নিয়মিত পর্যালোচনা করতে হবে।

## ৬.৪ এনক্রিপশন ব্যবস্থাপনা (Encryption Management)

সংবেদনশীল তথ্য সুরক্ষার জন্য শক্তিশালী ক্রিপ্টোগ্রাফি ব্যবহার বাধ্যতামূলক।

১. সব সংবেদনশীল ডেটা ট্রানজিট অবস্থায় TLS ১.২ বা তার উর্ধ্বতন প্রোটোকল ব্যবহার করে এনক্রিপ্ট করতে হবে।

২. গোপনীয় ডেটা (ডিস্ক, ডেটাবেস বা ক্লাউডে সংরক্ষিত) AES-২৫৬ বা সমমানের অ্যালগরিদম দিয়ে এনক্রিপ্ট করতে হবে।

৩. USB ড্রাইভ বা পোর্টেবল মিডিয়া এনক্রিপ্টেড হতে হবে, অন্যথায় নিষিদ্ধ।

৪. এনক্রিপশন কি নিরাপদভাবে সংরক্ষণ ও ব্যবস্থাপনা করতে হবে (যেমন: HSM বা Key Vault)।

৫. এনক্রিপশন সলিউশন টেস্ট করে কার্যকারিতা ও সামঞ্জস্য যাচাই করতে হবে।

৬. এই ব্যবস্থা অভ্যন্তরীণ সিস্টেম, ক্লাউড অ্যাপ্লিকেশন ও তৃতীয় পক্ষীয় ইন্টিগ্রেশনের ক্ষেত্রে প্রযোজ্য।

## ৬.৫ কর্মীদের দায়িত্ব ও আচরণবিধি (Employee Responsibilities and Code of Conduct)

কর্মকর্তা/কর্মচারী ও ভেন্ডাররা নিরাপত্তা বজায় রাখতে গুরুত্বপূর্ণ ভূমিকা পালন করে। এজন্য একটি আনুষ্ঠানিক সিকিউরিটি কোড অব কন্ডাক্ট প্রণয়ন করতে হবে। এতে অন্তর্ভুক্ত থাকবে—

১. মন্ত্রণালয়ের তথ্য, সিস্টেম ও ক্রিডেনশিয়াল অননুমোদিত প্রবেশ বা ফাঁস থেকে সুরক্ষিত রাখা;

২. কোনো সন্দেহজনক ইমেইল/ফিশিং, ম্যালওয়্যার সংক্রমণ, ডেটা ব্রিচ বা সন্দেহজনক কার্যকলাপ হলে তাৎক্ষণিকভাবে রিপোর্ট করা;

৩. প্রবেশাধিকার নিয়ন্ত্রণ (Access Control), সম্পদ ব্যবহার (Asset Usage), তথ্য পরিচালনা (Data Handling) ইত্যাদিসহ এই নির্দেশিকায় বর্ণিত সকল নিরাপত্তা নির্দেশনা যথাযথভাবে অনুসরণ করতে হবে;

৪. প্রতি বছর অন্তত একবার সাইবার নিরাপত্তা সচেতনতা প্রশিক্ষণে অংশগ্রহণ করা;

৫. অনুমোদন ছাড়া সফটওয়্যার ইনস্টল বা সিস্টেম কনফিগারেশন পরিবর্তন না করা;

৬. মন্ত্রণালয়ের সিস্টেম কোনো ব্যক্তিগত লাভ, হয়রানি বা অনৈতিক কাজে ব্যবহার না করা।

## ৭. প্রবেশাধিকার নিয়ন্ত্রণ (Access Control)

কার্যকর প্রবেশাধিকার নিয়ন্ত্রণ নিশ্চিতকরণের মাধ্যমে শুধুমাত্র অনুমোদিত ব্যবহারকারীরাই তাদের দায়িত্ব অনুযায়ী প্রয়োজনীয় সিস্টেম বা ডেটায় প্রবেশ করতে পারবে। দুর্বল প্রবেশাধিকার ব্যবস্থা তথ্যফাঁস/ডেটা ব্রিচ, সিস্টেম অপব্যবহার ও ইনসাইডার হুমকির মূল কারণ। ভূমি মন্ত্রণালয়ের ব্যবহৃত সকল সিস্টেম, অ্যাপ্লিকেশন ও প্ল্যাটফর্মে প্রবেশাধিকার নিয়ন্ত্রণ কার্যকর করতে প্রযোজ্য ব্যবস্থাপনা ও নিয়ন্ত্রণসমূহ উল্লেখ থাকা প্রয়োজন।

### ৭.১ ব্যবহারকারীর প্রবেশাধিকার জীবনচক্র ব্যবস্থাপনা (User Access Lifecycle Management)

একটি মানসম্মত User Access Lifecycle প্রক্রিয়া অনুসরণ করতে হবে, যেখানে অ্যাকাউন্ট তৈরি, পরিবর্তন ও নিষ্ক্রিয়করণ নিয়মিতভাবে নিয়ন্ত্রিত হবে।

#### ৭.১.১ Onboarding (নতুন ইউজার):

১. নতুন প্রবেশাধিকার আবেদনের অনুমোদন দিতে হবে সংশ্লিষ্ট দপ্তর প্রধানকে এবং সংশ্লিষ্ট সেবা প্রদানকারী দপ্তর/দায়িত্ব প্রাপ্ত কর্মকর্তা/কর্মচারী তা যাচাই করবে।

২. ব্যবহারকারী অ্যাকাউন্ট তৈরির আগে ব্যবহারকারীর ভূমিকা (User Roles) নির্ধারণ করতে হবে এবং কর্মসম্পাদনের জন্য Least Privilege Principle অনুসরণে যতটুকু প্রয়োজন ঠিক ততটুকুর সর্বনিম্ন অ্যাক্সেস প্রদান করতে হবে।

#### ৭.১.২ Modification (পরিবর্তন):

১. দায়িত্ব ও কর্তব্য পরিবর্তন হলে ব্যবহারকারীর প্রবেশাধিকার অবশ্যই পর্যালোচনা করে হালনাগাদ করতে হবে।

২. উচ্চস্তরের (Elevated) প্রবেশাধিকার অনুরোধগুলো অবশ্যই যৌক্তিক হতে হবে, নথিভুক্ত করতে হবে এবং নির্ধারিত কর্তৃপক্ষের অনুমোদন গ্রহণ করতে হবে।

#### ৭.১.৩ Offboarding (ইউজার নিষ্ক্রিয়করণ):

১. কোনো কর্মকর্তা/কর্মচারী পদত্যাগ, চাকরিচ্যুতি বা চুক্তির মেয়াদ শেষ হলে তার ব্যবহারকারী অ্যাকাউন্ট ২৪ ঘণ্টার মধ্যে নিষ্ক্রিয় করতে হবে।
২. কর্মকর্তা/কর্মচারীর অনুকূলে ইস্যুকৃত সব আইটি সম্পদ (IT assets) পুনরুদ্ধার করতে হবে এবং VPN ও ইমেইল অ্যাক্সেস দ্রুত বাতিল করতে হবে।
৩. সম্পূর্ণ ডি-প্রভিশনিং সম্পন্ন হয়েছে কিনা তা নিশ্চিত করতে Exit Access Review করতে হবে।
৪. সকল অ্যাক্সেস অনুরোধ ও পরিবর্তনসমূহ হেল্পডেস্ক/টিকিটিং সিস্টেমের মাধ্যমে ট্র্যাক করতে হবে যেন অডিটের জন্য প্রয়োজনীয় তথ্য পাওয়া যায়।

### ৭.২ ভূমিকা-ভিত্তিক প্রবেশাধিকার নিয়ন্ত্রণ (Role-Based Access Control - RBAC)

RBAC মডেল অনুসারে সিস্টেম এবং ডেটায় অ্যাক্সেস প্রদান করতে হবে, যেখানে স্পষ্টভাবে নির্ধারিত কর্মক্ষেত্রে ভূমিকার ভিত্তিতে ব্যবহারকারী অনুমতি নিয়ন্ত্রিত হবে।

১. প্রতিটি ব্যবহারকারীকে একটি নির্দিষ্ট ভূমিকায় (Role) চিত্রায়িত করতে হবে এবং প্রতিটি ভূমিকার জন্য পূর্বনির্ধারিত অ্যাক্সেস প্রোফাইল এর ব্যবস্থা থাকবে।

২. ভূমিকা (Roles) নিয়মিতভাবে পর্যালোচনা করতে হবে যেন সেগুলো বর্তমান দায়িত্বের সাথে সামঞ্জস্যপূর্ণ থাকে।

৩. কাস্টম বা ব্যতিক্রমধর্মী (Exception) ভূমিকা তৈরি কঠোরভাবে নিয়ন্ত্রিত হবে এবং যথাযথভাবে নথিভুক্ত করতে হবে।

৪. সম্ভব হলে অ্যাক্সেস প্রদান (Provisioning) স্বয়ংক্রিয়ভাবে সম্পন্ন করতে হবে যেমন: ডিরেক্টরি সার্ভিস বা Identity and Access Management (IAM) টুল ব্যবহার করা যেতে পারে।

৫. RBAC পদ্ধতি ব্যবহার করলে Privilege Creep (সময়ের পরিক্রমায় জমে যাওয়া অপ্রয়োজনীয় অতিরিক্ত অনুমতি) হ্রাসে সহায়তা করে এবং অ্যাক্সেস রিভিউ বা অডিটকে সহজ করে।

### ৭.৩ প্রিভিলেজড অ্যাক্সেস ম্যানেজমেন্ট (Privileged Access Management - PAM)

Privileged accounts (যেমন: সিস্টেম অ্যাডমিনিস্ট্রেটর, ডেটাবেস অ্যাডমিন, Root ইউজার) অপব্যবহার হলে তা একটি **গুরুত্বপূর্ণ নিরাপত্তা ঝুঁকি** তৈরি করে। তাই মন্ত্রণালয়কে অবশ্যই কঠোর **Privileged Access Management (PAM)** নিয়ন্ত্রণ বাস্তবায়ন করতে হবে, যার মধ্যে অন্তর্ভুক্ত হবে:

১. উচ্চস্তরের (Elevated) প্রবেশাধিকার প্রাপ্ত অ্যাডমিনিস্ট্রেটিভ ইউজার ও সাধারণ ইউজারদের জন্য আলাদা অ্যাকাউন্ট ব্যবহার করতে হবে।

২. নিরাপদ, ভল্ট-ভিত্তিক সমাধান ব্যবহার করা Privileged credentials সংরক্ষণ ও নিয়মিত পরিবর্তন করতে হবে।

৩. সব Privileged অ্যাকাউন্টে মাল্টি-ফ্যাক্টর অথেন্টিকেশন (MFA) সক্রিয় করতে হবে।

৪. সকল Privileged সেশন ও কার্যক্রমের লগ ব্যবস্থাপনা এবং মনিটরিংসহ সংবেদনশীল কমান্ডের জন্য রিয়েল-টাইম সতর্কতা নিশ্চিত করতে হবে।

৫. Privileged অ্যাকাউন্টধারীর সংখ্যা সীমিত রাখতে হবে এবং প্রতি ৩ মাসে পর্যালোচনার কার্যক্রম পরিচালনা করতে হবে।

৬. সকল জরুরি বা Break-Glass Access অবশ্যই সময়াবদ্ধ, অডিটযোগ্য এবং পরবর্তীতে অনুমোদিত হতে হবে।

### ৭.৪ প্রবেশাধিকার রিভিউ ও ডিপ্রভিশনিং (Access Review and De-Provisioning)

সময়ের সাথে সাথে এক্সেস সঠিক আছে কিনা তা নিশ্চিত করতে নিয়মিত পর্যালোচনা করতে হবে।

১. প্রতি ৬ মাসে অন্তত একবার (সংবেদনশীল সিস্টেমের ক্ষেত্রে আরও ঘন ঘন) রিভিউ করতে হবে।

২. দপ্তর প্রধান ও সিস্টেমের মালিকদের তাদের অধীনস্থ ইউজারদের এক্সেস পুনর্মূল্যায়ন করতে হবে।

৩. অব্যবহৃত/অরফ্যানড অ্যাকাউন্ট দ্রুত সরাতে হবে।

৪. অস্থায়ী এক্সেস নির্ধারিত সময় শেষে বাতিল করতে হবে।

৫. রিভিউ রিপোর্ট ও অ্যাকশন লগ কমপ্লায়েন্সের জন্য সংরক্ষণ করতে হবে।

৬. IAM টুল ব্যবহার করলে রিভিউ প্রক্রিয়া আরও দ্রুত ও কার্যকর হবে।

### ৭.৫ লজিক্যাল অ্যাক্সেস কন্ট্রোল (Applications, OS, DB, Network, Endpoints)

প্রযুক্তির প্রতিটি স্তরে একইভাবে অ্যাক্সেস কন্ট্রোল প্রযোজ্য হবে।

১. Applications:

a. শক্তিশালী অথেন্টিকেশন ও সেশন টাইমআউট প্রয়োগ করতে হবে।
b. ফিচার/মডিউল ভিত্তিক RBAC প্রয়োগ করতে হবে।
c. অতিরিক্ত ব্যর্থ লগইন হলে অ্যাকাউন্ট লক করতে হবে (যেমন: সর্বোচ্চ ৩ বারের ব্যর্থতায় ১ ঘন্টার জন্য অ্যাকাউন্ট লক হবে)।

২. Operating Systems (OS):

a. অব্যবহৃত অ্যাকাউন্ট ও সার্ভিস বন্ধ করতে হবে।
b. এক্সেস ও Privilege Escalation-এর জন্য অডিট চালু রাখতে হবে।
c. Root/Sudo কেবল অনুমোদিত ইউজারদের প্রদান করতে হবে।

৩. Databases:

a. ডেটাবেস অ্যাক্সেস শুধু অ্যাপ্লিকেশন/রোল ভিত্তিক হতে হবে।
b. Query লগ ও Data schema এর পরিবর্তনসমূহ মনিটর করতে হবে।
c. এনক্রিপ্টেড কানেকশন ব্যবহার করতে হবে।
d. DB এর Audit Trail চালু রাখতে হবে এবং কমপক্ষে ৩ মাসের ডেটা সংরক্ষণ করতে হবে।

৪. Networks:

a. নেটওয়ার্ক সেগমেন্টেশন প্রয়োগ করতে হবে যেন গুরুত্বপূর্ণ সিস্টেম আলাদা করা যায় (যেমন: Production বনাম Test আলাদা)।
b. ফায়ারওয়াল রুল এবং অ্যাক্সেস কন্ট্রোল লিস্ট (ACL) ব্যবহার করে নেটওয়ার্ক ডিভাইসের অ্যাক্সেস সীমাবদ্ধ করতে হবে।
c. ইনবাউন্ড ও আউটবাউন্ড ট্রাফিক মনিটর করতে হবে এবং অস্বাভাবিক কার্যক্রম চিহ্নিত করতে হবে।

৫. Endpoints:

a. সকল এন্ডপয়েন্ট ডিভাইসে লগইন ক্রেডেনশিয়াল বাধ্যতামূলক এবং নির্দিষ্ট সময় পর্যন্ত নিষ্ক্রিয় থাকলে auto-lock হতে হবে।
b. USB/এক্সটার্নাল ড্রাইভের ব্যবহার অনুমোদিত প্রক্রিয়া অনুযায়ী সীমিত করতে হবে।
c. ওয়ার্কস্টেশনের Local Admin Rights থাকবে না, শুধুমাত্র স্পষ্টভাবে অনুমোদিত ক্ষেত্র ছাড়া।

## ৮. সিস্টেম ও নেটওয়ার্ক নিরাপত্তা (System and Network Security)

মন্ত্রণালয়ের আইটি অবকাঠামো (যেমন: সার্ভার, ডেটাবেস, নেটওয়ার্কিং যন্ত্রপাতি ও সিস্টেম কনফিগারেশন) সুরক্ষিত রাখা অত্যন্ত জরুরি যেন সেবাসমূহ চালু থাকে, ডেটার অখণ্ডতা বজায় থাকে এবং কার্যক্রম স্থিতিশীল থাকে। সিস্টেম ও নেটওয়ার্ককে অভ্যন্তরীণ ও বাহ্যিক হুমকি থেকে সুরক্ষিত রাখার জন্য মৌলিক নিরাপত্তার প্রয়োজনীয়তা রয়েছে।

### ৮.১ সিস্টেম হার্ডেনিং ও কনফিগারেশন ব্যবস্থাপনা (System Hardening and Configuration Management)

সকল সিস্টেমকে শিল্পের সর্বোত্তম চর্চা (Industry Best Practices) এবং নিরাপত্তা বেঞ্চমার্ক (যেমন: CIS Benchmarks) অনুসারে সুরক্ষিতভাবে কনফিগার করতে হবে যেন আক্রমণের সুযোগ (Attack Surface) কমানো যায় এবং নিম্নোক্ত বিষয়াদি অন্তর্ভুক্ত থাকে:

১. অপ্রয়োজনীয় সার্ভিস, পোর্ট এবং সফটওয়্যার কম্পোনেন্ট নিষ্ক্রিয় বা আনইনস্টল করতে হবে।

২. সিস্টেম ডিপ্লয়মেন্টে সিকিউর কনফিগারেশন টেমপ্লেট ব্যবহার করতে হবে।

৩. ফাইল, ফোল্ডার ও সিস্টেম লেভেলের অবজেক্টে কঠোর পারমিশন সেটিং পলেসি প্রয়োগ করতে হবে।

৪. অপ্রয়োজনীয় অ্যাডমিন ইন্টারফেস নিষ্ক্রিয় বা সীমিত রাখতে হবে।

৫. সব সার্ভারের জন্য বেসলাইন কনফিগারেশন ডকুমেন্ট তৈরি করতে হবে ও পরিবর্তনের সাথে আপডেট করতে হবে।

৬. অটোমেটেড টুল ব্যবহার করে নিয়মিত কনফিগারেশন অডিট করতে হবে।

৭. কনফিগারেশন পরিবর্তন Change Management Process এর মাধ্যমে অনুমোদন করতে হবে।

### ৮.২ প্যাচ ও দুর্বলতা ব্যবস্থাপনা (Patch and Vulnerability Management)

মন্ত্রণালয় একটি Patch ও Vulnerability Management প্রোগ্রাম চালু করবে যেন সিস্টেমগুলো নিয়মিত আপডেট হয় এবং পরিচিত ঝুঁকি (known exploits) থেকে সুরক্ষিত থাকে যায়, যার মূল কার্যক্রমসমূহ হবে:

১. সব সিস্টেম ও তাদের প্যাচ লেভেলের হালনাগাদ তালিকা সংরক্ষণ করতে হবে।

২. প্রতি মাসে OS, Middleware, Application-এর প্যাচ আপডেট করতে হবে।

৩. অন্তত প্রতি ৩ মাসে ও বড় পরিবর্তনের পর ভলনারেবিলিটি স্ক্যান চালাতে হবে।

৪. ভলনারেবিলিটিকে Common Vulnerability Scoring System (CVSS) স্কোর অনুযায়ী Critical/High/Medium/Low হিসেবে চিহ্নিত করতে হবে।

৫. সমাধানের সময়সীমা: Critical = ৭ দিন, High = ১৪ দিন, Medium = ৩০ দিন নির্ধারণ করতে হবে।

৬. ফলো-আপ স্ক্যান দিয়ে প্যাচ কার্যকারিতা যাচাই করতে হবে।

৭. ইন্টারনেট-ফেসিং বা ক্রিটিক্যাল অ্যাপ্লিকেশন চালিত সিস্টেমকে অগ্রাধিকার দিতে হবে।

## ৮.৩ নেটওয়ার্ক নিরাপত্তা স্থাপত্য (Network Security Architecture)

Defense-in-Depth পদ্ধতি ব্যবহার করে নেটওয়ার্ককে ভাগ, আলাদা ও মনিটর করতে হবে।

Defense-in-Depth আর্কিটেকচার গ্রহণ করতে হবে যেন নেটওয়ার্ক ট্রাফিক ও সার্ভিসগুলো সেগমেন্ট, আইসোলেট এবং মনিটর করা যায় যেখানে নিম্নোক্ত বিষয়াদি অন্তর্ভুক্ত থাকবে:

১. নেটওয়ার্ক জোন আলাদা করা (Internal, DMZ, External, Test, Production) এবং ফায়ারওয়াল বা VLAN ব্যবহার করে সুরক্ষিত করতে হবে।

২. সংবেদনশীল অ্যাপ্লিকেশন ও ডেটা স্টোর আলাদা রাখতে জোনিং ব্যবস্থার প্রয়োগ করতে হবে।

৩. সকল পাবলিক-ফেসিং সার্ভারকে Reverse Proxy বা Web Application Firewalls (WAF) দিয়ে সুরক্ষিত করতে হবে।

৪. ফায়ারওয়াল/রাউটারে কঠোর inbound ও outbound রুল প্রয়োগ করতে হবে।

৫. গুরুত্বপূর্ণ স্থানে Intrusion Detection/Prevention Systems (IDS/IPS) স্থাপন করতে হবে।

৬. নেটওয়ার্ক ডিজাইন প্রতি বছর বা বড় পরিবর্তনের পর অথবা কোনো অবকাঠামোগত পরিবর্তনের পর পর্যালোচনা করতে হবে।

## ৮.৪ ফায়ারওয়াল ও পেরিমিটার কন্ট্রোলস (Firewall and Perimeter Controls)

ফায়ারওয়াল অননুমোদিত প্রবেশ ঠেকানোর জন্য সবচেয়ে গুরুত্বপূর্ণ নিয়ন্ত্রণ।

১. সব ইন্টারনেট গেটওয়ে ও নেটওয়ার্ক সীমান্তে ফায়ারওয়াল বসাতে হবে।

২. ফায়ারওয়াল রুলবুক নথিভুক্ত করতে হবে (পোর্ট, প্রোটোকল, IP Range ও ব্যবসায়িক কারণসহ)।

৩. প্রতি ৬ মাসে বা বড় ইনসিডেন্ট/পরিবর্তনের পর রুল রিভিউ/পর্যালোচনা করতে হবে।

৪. ফায়ারওয়ালে লগিং চালু রাখতে হবে এবং SIEM-এ ইন্টিগ্রেট করতে হবে।

৫. Next-Gen Firewall (NGFW) বা সমমানের প্রযুক্তি ব্যবহার করতে হবে।

৬. কোনো ভেন্ডর অফিস বা ডেভেলপমেন্ট এনভায়রনমেন্ট ফায়ারওয়াল ছাড়া চলতে পারবে না।

## ৮.৫ নেটওয়ার্ক বিভাজন (Network Segmentation)

ল্যাটারাল মুভমেন্ট ও অননুমোদিত এক্সেস রোধে নেটওয়ার্ককে ভাগ করতে হবে।

১. Production, Development, Test ও Admin নেটওয়ার্কের জন্য আলাদা VLAN এর ব্যবস্থা রাখতে হবে।

২. সেগমেন্টগুলোর মধ্যে কড়া ACL ও ফায়ারওয়াল রুল প্রয়োগ করতে হবে।

৩. ব্যবহারকারী ডিভাইসগুলোকে ব্যাকএন্ড সার্ভার ও ডেটাবেস থেকে আলাদা রাখতে হবে।

৪. ভেন্ডর ও তৃতীয় পক্ষকে শুধুমাত্র প্রয়োজনীয়তার ভিত্তিতে আলাদা পরিবেশে সীমিত অ্যাক্সেস প্রদান করতে হবে।

৫. Test ও Live সিস্টেম কোনো শেয়ার্ড/একই Subnet-এ থাকতে পারবে না।

৬. নেটওয়ার্ক ডায়াগ্রাম এবং সেগমেন্টেশন সম্পর্কিত ডকুমেন্ট নিয়মিত হালনাগাদ ও রিভিউ করতে হবে।

### ৮.৬ নিরাপদ রিমোট কানেক্টিভিটি (Secure Remote Connectivity)

দূর থেকে কাজ ও তৃতীয় পক্ষের সহযোগিতার ওপর নির্ভরশীলতা বৃদ্ধির কারণে নিরাপদ রিমোট অ্যাক্সেস অপরিহার্য বিধায় নিম্নলিখিত নিয়মাবলী প্রয়োগ করতে হবে:

১. সকল রিমোট সংযোগ অবশ্যই VPN এবং মাল্টি-ফ্যাক্টর অথেন্টিকেশন (MFA) ব্যবহার করে স্থাপন করতে হবে।

২. VPN সেশনগুলো সময়াবদ্ধ হতে হবে, Idle Timeout প্রয়োগ করে লগিং সক্রিয় রাখতে হবে।

৩. রিমোট ইউজারের সিস্টেমে বাধ্যতামূলকভাবে কমপ্লায়েন্স চেক (OS Patch Level, Antivirus Status) করতে হবে।

৪. পাবলিক নেটওয়ার্কে প্রশাসনিক অ্যাক্সেস (যেমন: SSH, RDP) শুধুমাত্র হোয়াইটলিস্টেড IP ঠিকানায় সীমাবদ্ধ রাখতে হবে এবং Jump Server বা Bastion Host ব্যবহার করতে হবে।

৫. স্ক্রিন শেয়ারিং এবং রিমোট কন্ট্রোল টুল অনুমোদিত হতে হবে এবং সেশন রেকর্ডিং সক্রিয় থাকতে হবে।

৬. রিমোট এক্সেস লগ সংরক্ষণ এবং অস্বাভাবিক কার্যক্রমের জন্য নিয়মিত পর্যালোচনা করতে হবে।

## ৯. এন্ডপয়েন্ট ও ওয়ার্কস্টেশন নিরাপত্তা (Endpoint and Workstation Security)

এন্ডপয়েন্ট ডিভাইস যেমন ডেস্কটপ, ল্যাপটপ ও পোর্টেবল ডিভাইসগুলো প্রায়শই ম্যালওয়ার, অননুমোদিত প্রবেশ ও ডেটা চুরির লক্ষ্যবস্তু হয়। তাই এগুলোতে সঠিক নিরাপত্তা কনফিগারেশন ও মনিটরিং থাকা অত্যন্ত জরুরি। এই অধ্যায়ে ভূমি মন্ত্রণালয় ও এর ভেন্ডর/কন্ট্রাক্টরের ব্যবহৃত সব এন্ডপয়েন্ট সুরক্ষার জন্য প্রয়োজনীয় নিয়ন্ত্রণসমূহ বর্ণনা করা হলো।

### ৯.১ লাইসেন্সকৃত সফটওয়্যার ব্যবহার (Licensed Software Enforcement)

শুধুমাত্র বৈধ ও ভেন্ডর-সাপোর্টেড সফটওয়্যার ব্যবহার করতে হবে।

১. মন্ত্রণালয়ের সব ওয়ার্কস্টেশন ও ভেন্ডার ডিভাইসে আসল লাইসেন্সকৃত OS ও সফটওয়্যার ইনস্টল করতে হবে এবং নিয়মিত আপডেট রাখতে হবে।

২. পাইরেটেড, মেয়াদোত্তীর্ণ বা সাপোর্টবিহীন সফটওয়্যার ব্যবহার সম্পূর্ণ নিষিদ্ধ।

৩. আইসিটি বিভাগ সব ডিভাইসের জন্য একটি কেন্দ্রীয় সফটওয়্যার ইনভেন্টরি রাখবে।

৪. কেবল অনুমোদিত সফটওয়্যার ইনস্টল করা যাবে; ব্যতিক্রম হলে লিখিত অনুমোদন প্রয়োজন।

৫. ভেন্ডরদের ব্যবহৃত টুল/প্ল্যাটফর্মের লাইসেন্স প্রমাণ জমা দিতে হবে।

### ৯.২ এন্ডপয়েন্ট প্রোটেকশন ও অ্যান্টিভাইরাস (Endpoint Protection and Antivirus)

সব এন্ডপয়েন্ট ডিভাইসে আধুনিক নিরাপত্তা সলিউশন থাকতে হবে।

১. NGAV (Next-Gen Antivirus) ব্যবহার করতে হবে, যা পরিচিত ও অচেনা হুমকি শনাক্ত করতে পারে;

২. রিয়েল-টাইম মনিটরিং সক্রিয় থাকতে হবে (যেমন: ফাইললেস আক্রমণ বা র‍্যানসমওয়্যার চিহ্নিত করা);

৩. থ্রেট অ্যালার্টগুলো কেন্দ্রীভূত SIEM প্ল্যাটফর্মে পাঠাতে হবে;

৪. প্রতিদিন সিগনেচার আপডেট এবং অন্তত সাপ্তাহিক ফুল স্ক্যান করতে হবে;

৫. অ্যান্টি-ম্যালওয়ার নিয়ন্ত্রণ ব্যবস্থা কেন্দ্রীয়ভাবে বাস্তবায়ন করতে হবে;

৬. USB ব্যবহারের আগে অটো-স্ক্যান করতে হবে (যদি অনুমোদিত হয়);

৭. ম্যালওয়ার শনাক্ত হলে ডিভাইস তাৎক্ষণিকভাবে আইসোলেট করতে হবে এবং ফরেনসিক তদন্ত চালাতে হবে।

### ৯.৩ ইউএসবি নিয়ন্ত্রণ (USB Controls)

রিমুভেবল মিডিয়া ম্যালওয়ার বা ডেটা লিকের প্রধান মাধ্যম হতে পারে। এজন্য—

১. সব ডেস্কটপ/ল্যাপটপে USB পোর্ট ডিফল্টভাবে বন্ধ রাখতে হবে; প্রয়োজন হলে লিখিত অনুমোদন নিয়ে চালু করা যাবে।

২. কেবল সরকারি-প্রদত্ত বা অনুমোদিত এনক্রিপ্টেড USB ডিভাইস ব্যবহার করা যাবে।

৩. এক্সটার্নাল মিডিয়াতে ডেটা ট্রান্সফার লগ ও মনিটর করতে হবে, এবং কন্টেন্ট স্ক্যান করতে হবে।

৪. প্রিন্টার, কীবোর্ড, ওয়্যারলেস অ্যাডাপ্টার, ওয়েবক্যাম ব্যবহারের আগে অনুমোদন নিতে হবে এবং ইনভেন্টরিতে নথিভুক্ত করতে হবে।

৫. DLP (Data Loss Prevention) ব্যবহার করে অননুমোদিত ফাইল মুভমেন্ট ব্লক করতে হবে।

## ৯.৪ ডিস্ক এনক্রিপশন ও ডেটা সুরক্ষা (Disk Encryption and Data Protection)

সংবেদনশীল ডেটা সুরক্ষার জন্য সব এন্ডপয়েন্টে ডিস্ক-লেভেল এনক্রিপশন চালু রাখতে হবে।

১. সব ল্যাপটপ, মোবাইল ডিভাইস এবং শ্রেণিবদ্ধ ডেটা-অ্যাক্সেসকারী ডেস্কটপে Full Disk Encryption (যেমন: BitLocker, LUKS) চালু রাখতে হবে।

২. এনক্রিপশন কি নিরাপদভাবে সংরক্ষণ করতে হবে (পাসওয়ার্ড-ভিত্তিক বা হার্ডওয়্যার-ভিত্তিক সাপোর্ট)।

৩. ডিভাইস হারানো, চুরি বা বাতিলের ক্ষেত্রে এনক্রিপশন ডেটা চুরি প্রতিরোধ করবে।

৪. সংবেদনশীল ফাইল প্রয়োজনে ফাইল/ফোল্ডার লেভেল এনক্রিপশনেও সুরক্ষিত করতে হবে।

৫. ভেন্ডরদের ডিভাইসেও মন্ত্রণালয়ের মান অনুযায়ী এনক্রিপশন থাকতে হবে।

## ৯.৫ কেন্দ্রীয় ব্যবস্থাপনা ও ডিরেক্টরি সার্ভিসেস (Centralized Management and Directory Services)

সব এন্ডপয়েন্টের ওপর নিয়ন্ত্রণ, দৃশ্যমানতা ও নির্দেশনা প্রয়োগ নিশ্চিত করতে কেন্দ্রীয় ব্যবস্থাপনা প্রয়োজন।

১. সব অফিসিয়াল ওয়ার্কস্টেশনকে কেন্দ্রীয় ডিরেক্টরি সার্ভিসে (যেমন: Active Directory, LDAP) যুক্ত করতে হবে;

২. গ্রুপ পলিসির মাধ্যমে স্ক্রিন লক, সফটওয়্যার রেস্ট্রিকশন, পাসওয়ার্ড ব্যবস্থা ও প্যাচ ডেপ্লয়মেন্ট বাধ্যতামূলক করতে হবে;

৩. এন্ডপয়েন্ট ম্যানেজমেন্ট সলিউশন (যেমন: Microsoft Intune) ব্যবহার করে অ্যাসেট ট্র্যাকিং, রিমোট কনফিগারেশন ও লকডাউন করতে হবে;

৪. মোবাইল বা অফসাইট ডিভাইসে রিমোট ওয়াইপ ও জিওফেন্সিং সক্রিয় রাখতে হবে;

৫. লোকাল ইউজার কার্যক্রম, সফটওয়্যার ইনস্টলেশন ও কনফিগারেশন পরিবর্তনের অডিট লগ সংরক্ষণ করতে হবে।

## ১০. সোর্স কোড ও অ্যাপ্লিকেশন নিরাপত্তা (Source Code and Application Security)

ভূমি মন্ত্রণালয় নাগরিকদের জন্য গুরুত্বপূর্ণ সেবা দিতে কাস্টম-ডেভেলপড ওয়েব অ্যাপ্লিকেশন ও প্ল্যাটফর্মের ওপর ব্যাপকভাবে নির্ভর করে। তাই এসব অ্যাপ্লিকেশনের সোর্স কোডের অখণ্ডতা, গোপনীয়তা ও প্রাপ্যতা সুরক্ষিত রাখা অত্যন্ত জরুরি। ইন-হাউজ টিম ও তৃতীয় পক্ষের ভেন্ডর দ্বারা তৈরি সব অ্যাপ্লিকেশনের সোর্স কোড ব্যবস্থাপনা ও নিরাপত্তা ব্যবস্থাপনা এর প্রয়োজন রয়েছে।

### ১০.১ সোর্স কোড মালিকানা ও হেফাজত (Source Code Ownership and Custody)

মন্ত্রণালয় সব অ্যাপ্লিকেশনের সোর্স কোডের পূর্ণ নিয়ন্ত্রণ ও মালিকানা বজায় রাখবে।

১. ভেন্ডরদের তৈরি কোড নিয়মিতভাবে মন্ত্রণালয়ের নিয়ন্ত্রিত রিপোজিটরিতে জমা দিতে হবে;

২. ভেন্ডরদের রিপোজিটরিতে প্রবেশাধিকার দিতে হবে এবং তা নিয়মিত আপডেট করতে হবে;

৩. লাইভ সিস্টেমে সরাসরি কোড পরিবর্তন কঠোরভাবে নিষিদ্ধ; সব কোডকে ডেভেলপমেন্ট পাইপলাইনের মধ্য দিয়ে প্রদান করতে হবে;

৪. ভেন্ডরদের সাথে চুক্তিতে Escrow Agreement বা কোড হস্তান্তর ধারা থাকতে হবে;

৫. কোডবেসের সঙ্গে টেকনিক্যাল ডকুমেন্টেশন, আর্কিটেকচার ডায়াগ্রাম ও API রেফারেন্স রাখতে হবে;

৬. কোড মালিকানা না থাকলে ভেন্ডর-লক-ইন, অজানা দুর্বলতা ও কার্যক্রমের ঝুঁকি তৈরি হতে পারে।

### ১০.২ সিকিউর কোডিং গাইডলাইন (Secure Coding Guidelines)

সব কোডকে নিরাপদ কোডিং স্ট্যান্ডার্ড মেনে তৈরি করতে হবে।

১. ডেভেলপারদের OWASP Top ১০ ও OWASP Secure Coding Practices মেনে চলতে হবে;

২. ইনপুট ভ্যালিডেশন, আউটপুট এনকোডিং ও নিরাপদ সেশন হ্যান্ডলিং ডিফল্টভাবে থাকতে হবে;

৩. হার্ডকোডেড ক্রিডেনশিয়াল, ব্যাকডোর বা ডিবাগ ফিচার সম্পূর্ণভাবে নিষিদ্ধ;

৪. এরর মেসেজে কোনো সেনসিটিভ সিস্টেম তথ্য প্রকাশ করা যাবে না;

৫. সব লাইব্রেরি ও ডিপেনডেন্সি লাইসেন্সকৃত হতে হবে এবং ভলনারেবিলিটি স্ক্যান করা হবে;

৬. ডেভেলপারদের জন্য নিয়মিত Secure Coding Training বাধ্যতামূলক।

### ১০.৩ ভার্সন কন্ট্রোল ও পরিবর্তন ব্যবস্থাপনা (Version Control and Change Management)

সব অ্যাপ্লিকেশন কোড Git-এর মতো নিরাপদ Version Control System (VCS)-এ সংরক্ষিত হতে হবে।

১. প্রতিটি প্রজেক্টের জন্য আলাদা রিপোজিটরি থাকবে, যেখানে স্পষ্ট commit history, version tagging ও release notes থাকবে।

২. কেবল অনুমোদিত ব্যক্তিরাই কোড push করতে পারবে এবং সব commit নির্দিষ্ট ব্যক্তির নামে ট্রেসযোগ্য হতে হবে।

৩. সব পরিবর্তন merge হওয়ার আগে Peer Review ও অনুমোদন পেতে হবে।

৪. জরুরি পরিবর্তনের ক্ষেত্রে Rollback ও Retrospective Approval প্রক্রিয়া থাকতে হবে।

৫. রিপোজিটরি নিরাপদ পরিবেশে হোস্ট করতে হবে, যেখানে এক্সেস কন্ট্রোল, এনক্রিপশন ও লগিং সক্রিয় থাকবে।

৬. রিপোজিটরি নিয়মিতভাবে ব্যাকআপ করতে হবে এবং রেডানডেন্ট লোকেশনে সংরক্ষণ করতে হবে।

## ১০.৪ কোড রিভিউ ও অনুমোদন প্রক্রিয়া (Code Review and Approval Processes)

**কোড লাইভে ডেপ্লয় হওয়ার আগে আনুষ্ঠানিক রিভিউ প্রক্রিয়া থাকতে হবে।**

১. প্রতিটি পরিবর্তন বা নতুন ফিচারকে পিয়ার ডেভেলপার বা সিকিউরিটি টিম রিভিউ করবে।

২. রিভিউতে Authentication, Access Control, Encryption ও Logging-এর মতো ক্রিটিক্যাল অংশ যাচাই করতে হবে।

৩. রিভিউ ম্যানুয়াল ও অটোমেটেড টুল উভয়টি দিয়েই রিভিউ প্রক্রিয়া সম্পন্ন করতে হবে।

৪. সব মন্তব্য নথিভুক্ত ও সমাধান করার পরেই অনুমোদন দেওয়া হবে।

৫. রিভিউ রেজাল্ট কমিটের সঙ্গে আর্কাইভ করে অডিটের জন্য রাখতে হবে।

৬. কোনো কোড অনুমোদন ছাড়া লাইভে ডেপ্লয় করা যাবে না।

## ১০.৫ কোড রিলিজের নিরাপত্তা পরীক্ষা (Security Testing for Code Releases)

নতুন কোড বা অ্যাপ্লিকেশন রিলিজের আগে কঠোর নিরাপত্তা পরীক্ষা করতে হবে।

১. ডেভেলপমেন্ট চলাকালীন SAST (Static Application Security Testing) চালাতে হবে।

২. DAST (Dynamic Application Security Testing) করতে হবে স্টেজিং পরিবেশে।

৩. ডিপেনডেন্সি স্ক্যান চালাতে হবে (যেমন: OWASP Dependency-Check, Snyk)।

৪. বড় রিলিজ বা আর্কিটেকচারাল পরিবর্তনের আগে Penetration Testing করতে হবে।

৫. পাওয়া সমস্যাগুলো ট্র্যাক করতে হবে, অগ্রাধিকারের ভিত্তিতে সমাধান করতে হবে এবং রিভ্যালিডেট করতে হবে।

৬. সব সিকিউরিটি টেস্টের রিপোর্ট নথিভুক্ত ও সংরক্ষণ করতে হবে।

## ১১. ক্লাউড ও ডাটা সেন্টার নিরাপত্তা (Cloud and Data Center Security)

ভূমি মন্ত্রণালয়ের তথ্য-উপাত্ত, অ্যাপ্লিকেশন এবং ডিজিটাল সেবা ক্লাউড অবকাঠামো, জাতীয় ডাটা সেন্টার অথবা সরকার অনুমোদিত ডাটা সেন্টারে পরিচালিত হলে সেগুলোর গোপনীয়তা (Confidentiality), অখণ্ডতা (Integrity) এবং লভ্যতা (Availability) নিশ্চিত করার জন্য নিম্নোক্ত নিরাপত্তা ব্যবস্থা গ্রহণ করতে হবে।

### ১১.১ ক্লাউড শাসন ও কমপ্লায়েন্স (Cloud Governance and Compliance)

মন্ত্রণালয় কর্তৃক ব্যবহৃত সকল ক্লাউড সেবা সরকার অনুমোদিত নীতিমালা, আইন, বিধি এবং তথ্য নিরাপত্তা নির্দেশিকার সঙ্গে সামঞ্জস্যপূর্ণ হতে হবে।

নিম্নোক্ত বিষয়সমূহ নিশ্চিত করতে হবে-

১. শুধুমাত্র সরকার অনুমোদিত ক্লাউড বা জাতীয় ডাটা সেন্টার ব্যবহার করতে হবে;

২. ক্লাউড সেবা গ্রহণের পূর্বে নিরাপত্তা ঝুঁকি মূল্যায়ন (Cloud Risk Assessment) সম্পন্ন করতে হবে;

৩. Service Level Agreement (SLA)-এ নিরাপত্তা, গোপনীয়তা, ব্যাকআপ, লগ সংরক্ষণ, ইনসিডেন্ট রিপোর্টিং এবং সেবার ধারাবাহিকতা সম্পর্কিত শর্ত অন্তর্ভুক্ত করতে হবে;

৪. ক্লাউড পরিবেশে সংরক্ষিত সকল তথ্যের মালিকানা ভূমি মন্ত্রণালয়ের থাকবে।

### ১১.২ ক্লাউড নিরাপত্তা নিয়ন্ত্রণ (Cloud Security Controls)

১. সকল ক্লাউড ব্যবহারকারীর জন্য Multi-Factor Authentication (MFA) বাধ্যতামূলক হবে;

২. সকল Administrative Account-এ Privileged Access Management (PAM) ব্যবহার করতে হবে;

৩. Role-Based Access Control (RBAC) বাস্তবায়ন করতে হবে;

৪. Data at Rest এবং Data in Transit উভয় অবস্থায় এনক্রিপশন নিশ্চিত করতে হবে;

৫. Encryption Key নিরাপদভাবে সংরক্ষণ ও ব্যবস্থাপনা করতে হবে;

৬. ক্লাউড নিরাপত্তা কনফিগারেশন নিয়মিত পর্যালোচনা করতে হবে।

### ১১.৩ ক্লাউড পর্যবেক্ষণ ও লগ ব্যবস্থাপনা

১. সকল প্রশাসনিক কার্যক্রমের Audit Log সংরক্ষণ করতে হবে;

২. লগসমূহ SIEM বা সমমানের নিরাপত্তা পর্যবেক্ষণ ব্যবস্থার সাথে সমন্বিত করতে হবে;

৩. অস্বাভাবিক কার্যক্রম শনাক্ত হলে তাৎক্ষণিকভাবে তদন্ত করতে হবে;

৪. লগ কমপক্ষে ১ (এক) বছর অথবা প্রযোজ্য আইন অনুযায়ী সংরক্ষণ করতে হবে।

### ১১.৪ ব্যাকআপ ও দুর্যোগ পুনরুদ্ধার

১. নিয়মিত ব্যাকআপ গ্রহণ করতে হবে;

২. ব্যাকআপ এনক্রিপ্টেড হতে হবে;

৩. Disaster Recovery (DR) পরিকল্পনা প্রণয়ন ও বছরে অন্তত একবার পরীক্ষা করতে হবে;

৪. Recovery Time Objective (RTO) এবং Recovery Point Objective (RPO) নির্ধারণ করতে হবে।

### ১১.৫ ক্লাউড ভেন্ডর ব্যবস্থাপনা

১. ক্লাউড সেবা প্রদানকারীর নিরাপত্তা সক্ষমতা নিয়মিত যাচাই করতে হবে;

২. চুক্তি সমাপ্তির পর সকল তথ্য নিরাপদভাবে প্রত্যাহার ও ধ্বংস নিশ্চিত করতে হবে;

৩. Vendor Exit Plan এবং Data Portability নিশ্চিত করতে হবে।

## ১২. নিরাপত্তা মনিটরিং ও অপারেশনস (Security Monitoring and Operations)

ভূমি মন্ত্রণালয়ের সিস্টেম ও ডেটা সুরক্ষার জন্য সক্রিয় ও ধারাবাহিক নিরাপত্তা মনিটরিং অপরিহার্য। এতে নেটওয়ার্ক কার্যক্রমে রিয়েল-টাইম দৃশ্যমানতা, অস্বাভাবিকতা শনাক্তকরণ, দ্রুত ইনসিডেন্ট রেসপন্স এবং নিয়মিত অভ্যন্তরীণ ও বাহ্যিক ইন্টেলিজেন্স সংগ্রহ অন্তর্ভুক্ত। নীচে মন্ত্রণালয়ের নিরাপত্তা ইভেন্ট শনাক্ত, প্রতিক্রিয়া ও পুনরুদ্ধারের জন্য নিয়ন্ত্রণ ও প্রক্রিয়াগুলো বর্ণনা করা হলো।

### ১২.১ SIEM ও লগ ম্যানেজমেন্ট (SIEM and Log Management)

মন্ত্রণালয়কে একটি কেন্দ্রীয় SIEM (Security Information and Event Management) সিস্টেম ব্যবহার করতে হবে।

১. সার্ভার, ফায়ারওয়াল, এন্ডপয়েন্ট প্রোটেকশন, VPN, ডেটাবেস ও অ্যাপ্লিকেশনের লগ SIEM-এ পাঠাতে হবে।

২. **মনিটর করতে হবে: লগইন চেষ্টা, Privilege Escalation, ফায়ারওয়াল রুল পরিবর্তন, সিস্টেম ক্র্যাশ, ম্যালওয়্যার শনাক্তকরণ, ফাইল ইন্টিগ্রিটি অ্যালার্ট।**

৩. **লগ অন্তত ১ বছর সংরক্ষণ করতে হবে; কমপক্ষে ৯০ দিন অনলাইনে রাখতে হবে।**

৪. **লগ ট্যাম্পারিং বা মুছে ফেলা থেকে সুরক্ষিত রাখতে হবে।**

৫. **করেলেশন রুল ও বিহেভিয়ার অ্যানালিটিক্স ব্যবহার করে অস্বাভাবিক কার্যক্রম রিয়েল-টাইমে শনাক্ত করতে হবে।**

৬. **SIEM থেকে তৈরি অ্যালার্টগুলো যাচাই, তদন্ত ও প্রতিক্রিয়াসহ নথিভুক্ত করতে হবে।**

৭. **SIEM সিস্টেমের হেলথ চেক নিয়মিত চালাতে হবে।**

### ১২.২ ইনসিডেন্ট শনাক্তকরণ ও প্রতিক্রিয়া (Incident Detection and Response)

একটি Incident Response Plan (IRP) তৈরি করতে হবে।

১. কর্মীদের প্রশিক্ষণ দিতে হবে যাতে তারা ফিশিং, ম্যালওয়্যার বা অননুমোদিত প্রবেশ চিহ্নিত ও রিপোর্ট করতে পারে।

২. ইনসিডেন্টগুলো গুরুত্ব অনুযায়ী শ্রেণিবদ্ধ করতে হবে: Critical / High / Medium / Low।

৩. সাধারণ ইনসিডেন্টের জন্য প্রি-ডিফাইন্ড প্লেবুক ব্যবহার করতে হবে (যেমন: ডেটা ব্রিচ, DDoS, Insider Threat)।

৪. প্রতিক্রিয়ার সময়সীমা:

- Critical: তাৎক্ষণিক (১ ঘণ্টার মধ্যে)
- High: ৪ ঘণ্টার মধ্যে
- Medium: ২৪ ঘণ্টার মধ্যে

৫. ইনসিডেন্ট শেষে Root Cause Analysis করতে হবে এবং কন্ট্রোল উন্নয়ন করতে হবে।

৬. সব ইনসিডেন্ট Incident Register-এ লগ রাখতে হবে এবং প্রয়োজনে ম্যানেজমেন্ট ও রেগুলেটরকে জানাতে হবে।

৭. IRP অন্তত বছরে একবার টেবিলটপ বা সিমুলেশন এক্সারসাইজ দিয়ে টেস্ট করতে হবে।

## ১২.৩ এসকেলেশন ম্যাট্রিক্স ও SLA প্রয়োগ (Escalation Matrix and SLA Enforcement)

মন্ত্রণালয়কে একটি স্পষ্ট **Escalation Matrix** তৈরি করতে হবে।

১. কোন ধরনের ইনসিডেন্টে কাকে জানাতে হবে (যেমন: সিস্টেম মালিক, CISO, ভেন্ডর, লিগ্যাল টিম)।

২. প্রতিটি Severity লেভেলের জন্য যোগাযোগের মাধ্যম (ইমেইল, SMS, ফোন, সিকিউর পোর্টাল)।

৩. DR প্ল্যান চালু বা কর্তৃপক্ষকে জানাতে হলে অনুমোদনের প্রক্রিয়া ও সময়সীমা নির্ধারণ।

ভেন্ডর/সার্ভিস প্রোভাইডারদের জন্য SLA বাধ্যতামূলক:

১. Critical: ২৪ ঘণ্টায় সমাধান

২. High: ৩ কার্যদিবস

৩. Medium: ৭ কার্যদিবস

৪. ভেন্ডরের SLA পারফরম্যান্স ত্রৈমাসিকভাবে রিভিউ করতে হবে।

## ১২.৪ ডার্ক ওয়েব মনিটরিং (Dark Web Monitoring)

ডার্ক ওয়েবে ডেটা ফাঁস বা নতুন হুমকি শনাক্তের জন্য মনিটরিং করতে হবে।

১. থ্রেট ইন্টেলিজেন্স প্ল্যাটফর্ম বা থার্ড-পার্টি সার্ভিস ব্যবহার করে ডার্ক ওয়েব স্ক্যান করতে হবে।

২. মন্ত্রণালয়ের ইমেইল, সিস্টেম ক্রিডেনশিয়াল, নাগরিক তথ্য বা গোপন নথি শনাক্ত হলে অ্যালার্ট দিতে হবে।

৩. অ্যালার্ট যাচাই করে প্রয়োজন হলে তাৎক্ষণিক ইনসিডেন্ট রেসপন্স নিতে হবে।

৪. মনিটরিংয়ের আওতায় থাকতে হবে অ্যাপ API, ডেটাবেস, কর্মীর ক্রিডেনশিয়াল।

৫. Breach Indicator পেলে পাসওয়ার্ড রিসেট ও সিস্টেম অডিট করতে হবে।

৬. ডার্ক ওয়েব ফাইন্ডিংস মাসিক রিপোর্ট আকারে CISO-কে জমা দিতে হবে।

## ১২.৫ নিরাপত্তা সচেতনতা ও প্রশিক্ষণ (Security Awareness and Training)

মানুষ নিরাপত্তার সবচেয়ে গুরুত্বপূর্ণ স্তর। এজন্য সচেতনতা ও প্রশিক্ষণ কার্যক্রম চালাতে হবে।

১. বছরে একবার বাধ্যতামূলক প্রশিক্ষণ (ফিশিং, পাসওয়ার্ড ব্যবস্থাপনা, ডেটা হ্যান্ডলিং, ইনসিডেন্ট রিপোর্টিং)।

২. Privileged ইউজার ও সিস্টেম অ্যাডমিনদের জন্য আলাদা সেশন (সিকিউর কনফিগারেশন, মনিটরিং, Insider Threat) এর ব্যবস্থা রাখতে হবে এবং আন্তর্জাতিক মনের প্রশিক্ষণ প্রদান করতে হবে।

৩. সিস্টেম সিকিউরিটির দায়িত্বে নিয়োজিত কর্মকর্তা/কর্মচারীদের আন্তর্জাতিক মনের এক্সপার্ট প্রশিক্ষণ প্রদান করতে হবে।

৪. পোস্টার, ইমেইল, কুইজ ও Simulated Phishing Test এর মাধ্যমে সচেতনতা প্রচারণা।

৫. নতুন কর্মীদের অরিয়েন্টেশন প্রশিক্ষণ দিতে হবে এক্সেস পাওয়ার আগে।

৬. প্রশিক্ষণের রেকর্ড রাখতে হবে এবং বোঝাপড়ার স্তর যাচাই করতে হবে।

৭. নিরাপত্তা সংস্কৃতি দৈনন্দিন কাজের অংশ হিসেবে গড়ে তুলতে হবে।

## ১৩. নিরাপত্তা মূল্যায়ন ও টেস্টিং (Security Assessment and Testing)

নিয়মিত নিরাপত্তা মূল্যায়ন ও টেস্টিং খুবই গুরুত্বপূর্ণ, কারণ এর মাধ্যমে বোঝা যায় বিদ্যমান নিয়ন্ত্রণ কতটা কার্যকর, নতুন দুর্বলতা কোথায় আছে এবং নিরাপত্তা মানদণ্ড মানা হচ্ছে কিনা। এই অধ্যায়ে ভূমি মন্ত্রণালয়ের গুরুত্বপূর্ণ সিস্টেমগুলোর জন্য ভালনারেবিলিটি এসেসমেন্ট, পেনেট্রেশন টেস্টিং ও থার্ড-পার্টি যাচাইয়ের পদ্ধতি, সময়সীমা ও শাসন ব্যবস্থা তুলে ধরা হলো।

### ১৩.১ ভালনারেবিলিটি এসেসমেন্ট ও পেনেট্রেশন টেস্টিং (VAPT)

### Vulnerability Assessment (VA):

১. সব ইন্টারনেট-ফেসিং সিস্টেমে প্রতি ত্রৈমাসিকে (Quarterly) এবং ইন্টারনাল সিস্টেমে প্রতি ছয় মাসে (Bi-annually) চালাতে হবে।

২. অটোমেটেড স্ক্যানিং টুল দিয়ে পুরোনো সফটওয়্যার, মিসকনফিগারেশন ও মিসিং প্যাচ শনাক্ত করতে হবে।

৩. সব ফলাফল নথিভুক্ত, অগ্রাধিকারে সাজানো এবং সংশ্লিষ্ট টিমকে শেয়ার করতে হবে।

৪. সমস্যা সমাধানের পর পুনরায় স্ক্যান করতে হবে।

### Penetration Testing (PT):

১. বছরে অন্তত একবার বা বড় সিস্টেম পরিবর্তন/ডেপ্লয়মেন্টের পর করতে হবে।

২. Black-box, White-box, Gray-box মেথড ব্যবহার করতে হবে।

৩. ওয়েব অ্যাপ (e-Porcha, LMS, LDTAX), API, মোবাইল অ্যাপ ও অবকাঠামো টেস্টের আওতায় আনতে হবে।

৪. টেস্ট অবশ্যই বাস্তব আক্রমণের মতো হতে হবে এবং OWASP, PTES, NIST SP ৮০০-১১৫ মান অনুসরণ করতে হবে।

৫. কেবলমাত্র স্বাধীন, যোগ্য বা CREST-সার্টিফায়েড ভেন্ডর টেস্ট পরিচালনা করবে।

## ১৩.২ নিরাপত্তা টেস্টিং ব্যবস্থাপনা (Security Testing Management)

আনুষ্ঠানিক ব্যবস্থাপনা থাকতে হবে, যাতে অন্তর্ভুক্ত থাকবে—

১. কোন সিস্টেমে টেস্ট হবে এবং স্কোপ

২. টেস্টের সময়সীমা ও শর্ত (Go-live-এর আগে, বড় পরিবর্তনের পর)

৩. টেস্ট শুরুর আগে প্রি-অ্যাপ্রুভাল ও চেঞ্জ কন্ট্রোল প্রসেস

৪. টেস্ট চলাকালীন ডেটা সুরক্ষা, যাতে সেবা বন্ধ না হয়

৫. টেস্ট রেজাল্ট, রেমিডিয়েশন লগ ও অনুমোদনপত্র সংরক্ষণ

৬. অভ্যন্তরীণ বা বহিরাগত টেস্টারদের জন্য NDA সই বাধ্যতামূলক

৭. ব্যবস্থাপনাটি প্রতি বছর পর্যালোচনা ও Information Security Steering Committee কর্তৃক অনুমোদিত হতে হবে।

## ১৩.৩ টেস্টিংয়ের ফ্রিকোয়েন্সি ও স্কোপ (Testing Frequency and Scope)

| অ্যাসেট টাইপ | টেস্টিং ফ্রিকোয়েন্সি | স্কোপ এলিমেন্টস |
|---|---|---|
| ইন্টারনেট-ফেসিং অ্যাপ্লিকেশন | ত্রৈমাসিক (VA), বার্ষিক (PT) | ওয়েব, API, DB, লগইন ফ্লো, ডেটা এক্সপোজার রিস্ক |
| ইন্টারনাল অ্যাপ্লিকেশন | ছয় মাসে একবার | এক্সেস কন্ট্রোল, সেশন ম্যানেজমেন্ট, ইনপুট ভ্যালিডেশন |
| মোবাইল অ্যাপ (Android/iOS) | বার্ষিক | ডিভাইস স্টোরেজ, API সিকিউরিটি, অথেন্টিকেশন |
| নেটওয়ার্ক ডিভাইস ও ফায়ারওয়াল | বার্ষিক | কনফিগারেশন রিভিউ, ACLs, রাউটিং সিকিউরিটি |
| ক্লাউড ইনফ্রাস্ট্রাকচার | বার্ষিক বা বড় পরিবর্তনের পর | IAM, এক্সপোজড সার্ভিস, এনক্রিপশন, লগিং |
| থার্ড-পার্টি হোস্টেড সিস্টেম | SLA অনুযায়ী | ভেন্ডর কন্ট্রাক্টে নির্ধারিত, রিপোর্ট মন্ত্রণালয়ে জমা |

## ১৩.৪ রেমিডিয়েশনের পর টেস্টিং (Post-Remediation Testing)

- সমাধানের পর সিকিউরিটি টিম যাচাই করবে সমস্যা পুরোপুরি ঠিক হয়েছে কিনা।
- Critical/High দুর্বলতা পুনঃটেস্ট করতে হবে সর্বোচ্চ ১৫ কার্যদিবসের মধ্যে।

- ফলো-আপ রিপোর্টে “Resolved, Partially Resolved, Unresolved” স্ট্যাটাস দেখাতে হবে।
- বারবার পাওয়া গেলে Root Cause Analysis করে ম্যানেজমেন্টে এসকেলেট করতে হবে।
- রেমিডিয়েশন সময়সীমা মন্ত্রণালয়ের **Vulnerability Management Policy** অনুযায়ী হতে হবে।

## ১৩.৫ তৃতীয় পক্ষের নিরাপত্তা টেস্টিং শর্ত (Third-Party Security Testing Requirements)

- সব ভেন্ডরকে মন্ত্রণালয় বা এর মনোনীত পার্টনার দ্বারা টেস্টিং গ্রহণে সম্মত হতে হবে।
- টেস্টিং স্কোপে কাস্টম সফটওয়্যার, প্ল্যাটফর্ম ও ইন্টিগ্রেশন অন্তর্ভুক্ত থাকতে হবে।
- ভেন্ডর-হোস্টেড এনভায়রনমেন্ট Go-live এর আগে ও পরে নিয়মিত টেস্টের আওতায় আসতে হবে।
- রিপোর্ট ও রেমিডিয়েশন প্রমাণ জমা দিতে হবে।
- টেস্টিং অস্বীকার করলে CISO ও লিগ্যাল টিম এর অনুমোদন প্রয়োজন।
- সব ভেন্ডর চুক্তিতে টেস্টিং ধারা অন্তর্ভুক্ত থাকতে হবে।

## ১৪. কর্ম-সম্পাদন ধারাবাহিকতা ও দুর্যোগ পুনরুদ্ধার (Business Continuity and Disaster Recovery - BCDR)

নাগরিক সেবা অব্যাহত রাখা, নাগরিক তথ্য সুরক্ষিত রাখা এবং প্রাকৃতিক দুর্যোগ, সাইবার আক্রমণ বা সিস্টেম ব্যর্থতার সময়ও কার্যক্রম চালু রাখার জন্য ভূমি মন্ত্রণালয়কে একটি Business Continuity and Disaster Recovery (BCDR) প্রোগ্রাম বাস্তবায়ন করতে হবে। আইসিটি অপারেশনের ধারাবাহিকতা নিশ্চিত করা এবং গুরুত্বপূর্ণ সেবা দ্রুত পুনরুদ্ধারের জন্য পরিকল্পনা, বাস্তবায়ন ও রক্ষণাবেক্ষণের শর্তাবলি উল্লেখ থাকা জরুরি।

### ১৪.১ BCM ও DR ব্যবস্থাপনা (BCM and DR Management)

মন্ত্রণালয়কে একটি আনুষ্ঠানিক BCM এবং DR ব্যবস্থাপনা প্রণয়ন করতে হবে, যেখানে লক্ষ্য, দায়িত্ব ও প্রক্রিয়া নির্ধারণ থাকবে।

১. ব্যবস্থাপনাটি অবশ্যই ISO ২২৩০১:২০১৯ মানদণ্ডের সঙ্গে সামঞ্জস্যপূর্ণ হতে হবে;

২. সিনিয়র নেতৃত্ব কর্তৃক অনুমোদিত হতে হবে এবং অন্তত বছরে একবার রিভিউ করতে হবে;

৩. BCDR কো-অর্ডিনেটর, DR লিড, ব্যাকআপ অ্যাডমিনিস্ট্রেটরদের ভূমিকা স্পষ্টভাবে নির্ধারণ করতে হবে;

৪. কোন কোন ব্যাঘাত অন্তর্ভুক্ত থাকবে (আগুন, বন্যা, হার্ডওয়্যার ব্যর্থতা, র‍্যানসমওয়্যার, বিদ্যুৎ বিভ্রাট ইত্যাদি) তা উল্লেখ করতে হবে;

৫. নিয়মিত ড্রিল ও সক্ষমতা যাচাই করতে হবে প্রস্তুতি নিশ্চিত করার জন্য;

৬. BCM/DR ব্যবস্থাপনাকে মন্ত্রণালয়ের সামগ্রিক তথ্য নিরাপত্তা কাঠামোর সঙ্গে একীভূত করতে হবে।

### ১৪.২ ডেটা ও প্রক্রিয়ার তালিকা (Data and Process Inventory)

প্রয়োজনীয় সেবা চিহ্নিত করতে একটি Business Impact Analysis (BIA) ও হালনাগাদ ইনভেন্টরি বজায় রাখতে হবে।

১. গুরুত্বপূর্ণ অ্যাপ্লিকেশন ও সাপোর্টিং ইনফ্রাস্ট্রাকচার তালিকাভুক্ত করতে হবে।

২. সিস্টেম, ডেটা সেন্টার, নেটওয়ার্ক ও তৃতীয় পক্ষের সেবার মধ্যে নির্ভরশীলতা চিহ্নিত করতে হবে।

৩. অ্যাপ্লিকেশনগুলোকে Criticality, Availability, Data Sensitivity অনুযায়ী শ্রেণিবিন্যাস করতে হবে।

৪. প্রযুক্তি ব্যর্থ হলে বিকল্প ম্যানুয়াল প্রক্রিয়ার ব্যবস্থা রাখতে হবে।

৫. সিস্টেমের মালিক, সাপোর্ট টিম ও DR ভেন্ডরের যোগাযোগ তথ্য রাখতে হবে।

৬. এই ইনভেন্টরি প্রতি ৬ মাসে বা বড় প্রযুক্তিগত পরিবর্তনের পর রিভিউ করতে হবে।

## ১৪.৩ RTO/RPO নির্ধারণ (RTO/RPO Definitions)

প্রত্যেক গুরুত্বপূর্ণ অ্যাপ্লিকেশন ও সেবার জন্য Recovery Time Objective (RTO) ও Recovery Point Objective (RPO) নির্ধারণ করতে হবে।

- RTO = সর্বোচ্চ গ্রহণযোগ্য সময়, যার মধ্যে সেবা পুনরুদ্ধার করতে হবে।
- RPO = সর্বোচ্চ সময়সীমা, যতটা ডেটা হারানো মেনে নেওয়া যাবে।

| সিস্টেম | RTO | RPO |
|---|---|---|
| e-Mutation Portal | | |
| LD Tax System | | |
| Land Records Database | | |

এই মানগুলো অনুযায়ী ব্যাকআপ টেকনোলজি, রেপ্লিকেশন ইন্টারভাল এবং DR অবকাঠামো নির্বাচন করতে হবে।

## ১৪.৪ ব্যাকআপ ব্যবস্থাপনা ও যাচাই (Backup Management and Validation)

ডেটা হারানো, দুর্নীতি বা র‍্যানসমওয়্যার থেকে রক্ষা করতে নিয়মিত ব্যাকআপ গ্রহণ করতে হবে।

১. সব গুরুত্বপূর্ণ সিস্টেম ও ডেটাবেসে দৈনিক ব্যাকআপ, এবং সংবেদনশীল সিস্টেমে রিয়েল-টাইম/ইনক্রিমেন্টাল ব্যাকআপ রাখতে হবে।

২. ব্যাকআপ অফসাইট বা ক্লাউডে সংরক্ষণ করতে হবে এবং AES-২৫৬ বা সমমানের এনক্রিপশন ব্যবহার করতে হবে।

৩. Retention Policy: ব্যবসা ও নিয়ন্ত্রক চাহিদা অনুযায়ী (যেমন: অপারেশনাল = ৩ মাস, রেগুলেটরি = ৭ বছর)।

৪. ব্যাকআপ লগ প্রতিদিন পর্যবেক্ষণ করতে হবে এবং ব্যর্থ হলে তাৎক্ষণিক ব্যবস্থা নিতে হবে।

৫. প্রতি ৩ মাসে ব্যাকআপ রিস্টোরেশন টেস্ট করতে হবে।

৬. ব্যাকআপ সিস্টেম ও মিডিয়ায় প্রবেশাধিকার কঠোরভাবে নিয়ন্ত্রিত ও লগড হতে হবে।

৭. কোনো প্রোডাকশন পরিবেশ পরীক্ষিত ব্যাকআপ ছাড়া চলতে পারবে না।

## ১৪.৫ DR টেস্টিং ও পরিকল্পনা রক্ষণাবেক্ষণ (DR Testing and Plan Maintenance)

DR প্ল্যান নিয়মিত টেস্ট ও আপডেট করতে হবে কার্যকারিতা বজায় রাখতে।

১. টেবিলটপ এক্সারসাইজ চালাতে হবে বিভিন্ন পরিস্থিতি (আগুন, সাইবার আক্রমণ ইত্যাদি) অনুকরণ করে।

২. বছরে অন্তত একবার পূর্ণ DR ড্রিল করতে হবে, যেখানে ব্যাকআপ/ফেলওভার সিস্টেম থেকে সেবা পুনরুদ্ধার করা হবে।

৩. টেস্ট রিপোর্টে উল্লেখ করতে হবে: টেস্টকৃত সিস্টেম, RTO/RPO অর্জন, পাওয়া সমস্যা ও সমাধান।

৪. প্রতিটি টেস্ট বা বড় পরিবর্তনের পর DR প্ল্যান আপডেট করতে হবে।

৫. সংশ্লিষ্ট সবাইকে DR প্রক্রিয়ায় প্রশিক্ষণ দিতে হবে এবং যোগাযোগ তালিকা প্রতি ৩ মাসে আপডেট করতে হবে।

৬. DR প্ল্যান টেস্ট ও আপডেট না করলে জরুরি অবস্থায় এটি অকার্যকর হয়ে যেতে পারে।

## ১৫. প্রশিক্ষণ ও সচেতনতা (Training and Security Awareness)

ভূমি মন্ত্রণালয়ের সকল কর্মকর্তা, কর্মচারী, প্রকল্পভিত্তিক জনবল, পরামর্শক এবং ভেন্ডর প্রতিষ্ঠানের তথ্য নিরাপত্তা সচেতনতা বৃদ্ধি এবং নিরাপদ তথ্য ব্যবস্থাপনা নিশ্চিত করার লক্ষ্যে নিয়মিত প্রশিক্ষণ ও সচেতনতামূলক কার্যক্রম পরিচালনা করতে হবে।

### ১৫.১ নিরাপত্তা সচেতনতা

সকল কর্মকর্তা-কর্মচারীকে বছরে অন্তত একবার সাইবার নিরাপত্তা সচেতনতা প্রশিক্ষণে অংশগ্রহণ করতে হবে।

প্রশিক্ষণে অন্তর্ভুক্ত থাকবে-

- Password Security, Phishing ও Social Engineering, Email Security, Internet নিরাপত্তা, Data Classification, Data Privacy, Malware ও Ransomware, Mobile Device Security, USB নিরাপত্তা, Remote Working Security, AI ব্যবহারে নিরাপত্তা ইত্যাদি

### ১৫.২ আইসিটি কর্মীদের কারিগরি প্রশিক্ষণ

আইসিটি সেলের কর্মকর্তা ও সাইবার নিরাপত্তা সংশ্লিষ্ট কর্মীদের নিয়মিত কারিগরি প্রশিক্ষণ প্রদান করতে হবে।

যেমন-

- Network Security, Secure Coding, Digital Forensics, Incident Response, Vulnerability Assessment, Penetration Testing, Cloud Security, API Security, SIEM, Threat Hunting ইত্যাদি

### ১৫.৩ ভেন্ডর প্রশিক্ষণ

মন্ত্রণালয়ের তথ্য বা সিস্টেমে প্রবেশাধিকারপ্রাপ্ত সকল ভেন্ডর ও পরামর্শককে নিরাপত্তা নির্দেশিকা সম্পর্কে অবহিত করতে হবে এবং প্রয়োজনীয় প্রশিক্ষণ প্রদান করতে হবে।

### ১৫.৪ মহড়া (Simulation Exercise)

প্রতি বছর অন্তত একবার নিম্নোক্ত মহড়া পরিচালনা করতে হবে-

১. Cyber Incident Drill
২. Phishing Simulation
৩. Disaster Recovery Drill
৪. Table-top Exercise
৫. Business Continuity Exercise

### ১৫.৫ প্রশিক্ষণ রেকর্ড: প্রশিক্ষণ, অংশগ্রহণ, মূল্যায়ন এবং ফলাফল সংক্রান্ত রেকর্ড সংরক্ষণ করতে হবে।

## ১৬. উদীয়মান প্রযুক্তির নিরাপত্তা (Emerging Technology Security)

কৃত্রিম বুদ্ধিমত্তা (AI), Machine Learning (ML), Internet of Things (IoT), Robotic Process Automation (RPA), Blockchain, API এবং অন্যান্য উদীয়মান প্রযুক্তি ব্যবহারের ক্ষেত্রে তথ্য নিরাপত্তা, ব্যক্তিগত উপাত্তের সুরক্ষা এবং সরকারি তথ্যের গোপনীয়তা নিশ্চিত করতে হবে।

### ১৬.১ কৃত্রিম বুদ্ধিমত্তা (Artificial Intelligence)

AI ব্যবহার করার পূর্বে ঝুঁকি মূল্যায়ন করতে হবে।

নিম্নোক্ত বিষয় নিশ্চিত করতে হবে-

১. AI ব্যবহারের উদ্দেশ্য নথিভুক্ত করতে হবে।
২. সংবেদনশীল সরকারি তথ্য অনুমোদন ছাড়া কোনো পাবলিক AI প্ল্যাটফর্মে ব্যবহার করা যাবে না।
৩. AI-এর মাধ্যমে প্রাপ্ত ফলাফল দায়িত্বপ্রাপ্ত কর্মকর্তার মাধ্যমে যাচাই করতে হবে।
৪. AI কর্তৃক গৃহীত সিদ্ধান্তের চূড়ান্ত অনুমোদন মানব কর্তৃক প্রদান করতে হবে।

### ১৬.২ Machine Learning

১. প্রশিক্ষণ ডেটার নিরাপত্তা নিশ্চিত করতে হবে।
২. Model Poisoning প্রতিরোধে নিয়ন্ত্রণ ব্যবস্থা থাকতে হবে।
৩. মডেল নিয়মিত পর্যালোচনা ও যাচাই করতে হবে।

### ১৬.৩ API Security

ভূমি মন্ত্রণালয়ের বিভিন্ন ডিজিটাল সেবার মধ্যে তথ্য আদান-প্রদানের জন্য ব্যবহৃত API-এর নিরাপত্তা নিশ্চিত করতে হবে।

নিম্নোক্ত বিষয়সমূহ অনুসরণ করতে হবে-

১. Authentication
২. Authorization
৩. API Gateway
৪. Rate Limiting
৫. Encryption
৬. Logging
৭. API Key Rotation
৮. API Monitoring

## ১৬.৪ Internet of Things (IoT)

IoT ডিভাইস ব্যবহারের ক্ষেত্রে-

১. Default Password পরিবর্তন করতে হবে।
২. Firmware নিয়মিত আপডেট করতে হবে।
৩. Network Segmentation নিশ্চিত করতে হবে।
৪. Device Inventory সংরক্ষণ করতে হবে।

## ১৬.৫ Robotic Process Automation (RPA)

১. Bot Account পৃথকভাবে নিয়ন্ত্রণ করতে হবে।
২. সকল কার্যক্রম লগ করতে হবে।
৩. Bot Credential নিরাপদভাবে সংরক্ষণ করতে হবে।
৪. Bot-এর কার্যক্রম নিয়মিত পর্যালোচনা করতে হবে।

### ১৬.৬ সামাজিক যোগাযোগ মাধ্যম ও ভার্চুয়াল মিটিং

১. সরকারি তথ্য সামাজিক যোগাযোগ মাধ্যমে প্রকাশের পূর্বে অনুমোদন নিতে হবে।
২. অনুমোদিত Virtual Meeting Platform ব্যবহার করতে হবে।
৩. সংবেদনশীল সভার ক্ষেত্রে End-to-End Encryption এবং Waiting Room ব্যবহার করতে হবে।

### ১৬.৭ উদীয়মান প্রযুক্তির ঝুঁকি মূল্যায়ন

নতুন প্রযুক্তি বাস্তবায়নের পূর্বে নিম্নোক্ত মূল্যায়ন সম্পন্ন করতে হবে-

১. Cyber Risk Assessment
২. Privacy Impact Assessment (PIA)
৩. Security Testing
৪. Legal Compliance Review
৫. Third-Party Risk Assessment

## ১৭. কমপ্লায়েন্স, রিপোর্টিং ও নন-কমপ্লায়েন্স ব্যবস্থা (Compliance, Reporting and Non-Compliance Management)

### ১৭.১ কমপ্লায়েন্স (Compliance)

এই নির্দেশিকার আওতাভুক্ত সকল কর্মকর্তা-কর্মচারী, প্রকল্প, আইসিটি সেল, ভেন্ডর, পরামর্শক এবং তৃতীয় পক্ষকে এই নির্দেশিকার বিধানসমূহ অনুসরণ করতে হবে। নিয়মিতভাবে নির্দেশিকার বাস্তবায়ন যাচাই করতে হবে। প্রয়োজনে Self Assessment, Compliance Checklist, Security Verification সম্পন্ন করতে হবে।

### ১৭.২ পর্যবেক্ষণ ও রিপোর্টিং (Monitoring and Reporting)

আইসিটি সেল নিয়মিতভাবে নিরাপত্তা ঘটনার তথ্য, ঝুঁকি, দুর্বলতা, কমপ্লায়েন্স অবস্থা, গুরুত্বপূর্ণ পরিবর্তন সংক্রান্ত প্রতিবেদন প্রস্তুত করবে। প্রতিবেদন প্রয়োজন অনুযায়ী সিনিয়র সচিব/সচিব, দায়িত্বপ্রাপ্ত কর্তৃপক্ষ, সংশ্লিষ্ট কমিটি এর নিকট উপস্থাপন করা হবে।

### ১৭.৩ নিরাপত্তা ঘটনার রিপোর্টিং

যে কোনো Cyber Attack, Malware, Ransomware, Unauthorized Access, Data Leakage, System Failure তাৎক্ষণিকভাবে আইসিটি সেলকে অবহিত করতে হবে। প্রয়োজনে Government CIRT এবং সংশ্লিষ্ট কর্তৃপক্ষকে জানাতে হবে।

### ১৭.৪ যাচাইকরণ (Verification)

এই নির্দেশিকার বাস্তবায়ন নিয়মিত যাচাই করতে হবে। যাচাইকরণে অন্তর্ভুক্ত থাকবে Configuration Review, Access Review, Vulnerability Verification, Backup Verification, Log Review, Compliance Verification

### ১৭.৫ নন-কমপ্লায়েন্স ব্যবস্থাপনা

যদি কোনো কর্মকর্তা, কর্মচারী, ভেন্ডর বা তৃতীয় পক্ষ এই নির্দেশিকার বিধান অনুসরণে ব্যর্থ হন, তবে-

১. ঘটনা নথিভুক্ত করতে হবে;

২. ঝুঁকি মূল্যায়ন করতে হবে;

৩. প্রয়োজনীয় সংশোধনমূলক ব্যবস্থা (Corrective Action) গ্রহণ করতে হবে;

৪. নির্ধারিত সময়ের মধ্যে পুনরায় কমপ্লায়েন্স নিশ্চিত করতে হবে।

## ১৭.৬ ব্যতিক্রম অনুমোদন (Exception Management)

বিশেষ প্রয়োজন ব্যতীত এই নির্দেশিকার কোনো বিধান থেকে বিচ্যুতি গ্রহণযোগ্য হবে না। যদি কোনো ব্যতিক্রম প্রয়োজন হয় তবে-

১. লিখিত যৌক্তিকতা থাকতে হবে;

২. ঝুঁকি মূল্যায়ন সম্পন্ন করতে হবে;

৩. যথাযথ কর্তৃপক্ষের অনুমোদন নিতে হবে;

৪. নির্দিষ্ট সময়সীমা নির্ধারণ করতে হবে।

## ১৭.৭ ধারাবাহিক উন্নয়ন (Continuous Improvement)

এই নির্দেশিকা কমপক্ষে প্রতি ০২ (দুই) বছর অন্তর অথবা নিম্নোক্ত পরিস্থিতিতে পুনঃপর্যালোচনা করতে হবে-

১. নতুন আইন বা নীতিমালা প্রণীত হলে;

২. বড় ধরনের সাইবার নিরাপত্তা ঘটনা ঘটলে;

৩. নতুন প্রযুক্তি বাস্তবায়িত হলে;

৪. গুরুত্বপূর্ণ ঝুঁকি শনাক্ত হলে;

৫. মন্ত্রণালয়ের ব্যবসায়িক প্রয়োজন পরিবর্তিত হলে।

## ১৮. বিবিধ

### ১৮.১ নির্দেশ প্রদানের ক্ষমতা:

যদি কোনো গুরুত্বপূর্ণ বিষয় এই নির্দেশিকা অনুযায়ী বাস্তবায়ন করা সম্ভব না হয়, তাহলে সিনিয়র সচিব/সচিব, ভূমি মন্ত্রণালয় লিখিতভাবে কারণসহ ব্যাখ্যা দিয়ে নির্দেশ দিতে পারবেন। এমন নির্দেশ দেওয়া হলে সংশ্লিষ্ট ক্ষেত্র তা অনুসরণ করতে বাধ্য থাকবে।

### ১৮.২ অব্যাহতি:

সিনিয়র সচিব/সচিব বিশেষ পরিস্থিতিতে, নির্দিষ্ট পরিধি বা ক্ষেত্রে নির্দিষ্ট সময়ের জন্য এই নির্দেশিকার কোনো বিধান প্রয়োগ থেকে শর্ত সাপেক্ষে অব্যাহতি দিতে পারে।

### ১৮.৩ নির্দেশিকার সীমাবদ্ধতা:

(১) এই নির্দেশিকার আওতায় থাকা দপ্তরগুলো তাদের নিজ নিজ ক্ষেত্রের জন্য সাইবার নিরাপত্তা, আইসিটি নীতি, পরিকল্পনা এবং অতিরিক্ত নিরাপত্তা ব্যবস্থা বাস্তবায়ন করতে পারবে। সেই ক্ষেত্রে এই নির্দেশিকা কেবল সহায়ক হিসেবে গণ্য হবে।

(২) এই নির্দেশিকার আরেকটি লক্ষ্য হলো, অন্তর্ভুক্ত ক্ষেত্রগুলোতে ন্যূনতম নিরাপত্তা নিশ্চিত করতে সংগঠনকে প্রয়োজনীয় সরঞ্জাম ও পদ্ধতির প্রাথমিক দিকনির্দেশনা প্রদান।

(৩) প্রযুক্তিগত পরিবর্তন, নতুন জ্ঞান বা বাস্তব অভিজ্ঞতার ভিত্তিতে নির্দেশিকাটি নিয়মিত হালনাগাদ করা যাবে।

গুরুত্বপূর্ণ শব্দকোষ এবং সংক্ষিপ্ত রূপ

| Term/Abbreviation | Definition |
|---|---|
| CIA | Confidentiality, Integrity, and Availability – the core pillars of information security |
| ISMS | Information Security Management System |
| RBAC | Role-Based Access Control – access based on job role or function |
| PAM | Privileged Access Management – managing elevated user rights |
| SIEM | Security Information and Event Management – central log collection and analysis |
| DR | Disaster Recovery – recovery of systems after disruption or failure |
| BCP | Business Continuity Plan – strategy to ensure uninterrupted operations during crises |
| PoLP | Principle of Least Privilege – users are given minimum necessary access |
| MFA | Multi-Factor Authentication – security requiring multiple verification factors |