গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

খসড়া

জাতীয় ডাটা সেন্টার ক্লাউড কম্পিউটিং নীতিমালা ২০২৩ (খসড়া)

Bangladesh Computer Council

Information and Communication Technology Division

NATIONAL DATA CENTER BANGLADESH

১. পটভূমি

তথ্য ও যোগাযোগ প্রযুক্তির (আইসিটি) সর্বোচ্চ ব্যবহার নিশ্চিত করিয়া সমাজের সকল শ্রেণি পেশার মানুষের জীবনমানে ইতিবাচক পরিবর্তন সাধনের মাধ্যমে জ্ঞানভিত্তিক উন্নত বাংলাদেশ গড়ে তোলা মাননীয় প্রধানমন্ত্রী শেখ হাসিনার অন্যতম রাজনৈতিক অঙ্গীকার। ২০০৮ সালে নবম জাতীয় সংসদ নির্বাচনের পূর্বে মাননীয় প্রধানমন্ত্রী শেখ হাসিনা আওয়ামী লীগের নির্বাচনী ইশতেহার 'দিন বদলের সনদ'-এ "২০২১ সালের মধ্যে ডিজিটাল বাংলাদেশ" গড়ে তোলার ঘোষণা দেন। এরই ধারাবাহিকতায় 'ডিজিটাল বাংলাদেশ' গড়ার পথ পেরিয়ে সরকার এখন স্মার্ট বাংলাদেশ গড়ার পথে চলতে শুরু করেছে।

স্মার্ট বাংলাদেশে উত্তরনের নবযাত্রায় সরকারি ও বেসরকারি পর্যায়ে ডিজিটাইজেশন ও সার্ভিস অটোমেশন দ্রুত বিকশিত হচ্ছে। প্রযুক্তির উৎকর্ষতায় ক্রমবর্ধমান ডিজিটাল কার্যক্রমে ডাটা সেন্টারের ব্যবহার বৃদ্ধি পাচ্ছে। ডাটা সেন্টার স্থাপন ও রক্ষণাবেক্ষণ, পরিচালন ব্যয়, নতুন প্রযুক্তি ব্যবহারের চাহিদা, Total Cost of Ownership (TCO) ইত্যাদি বিবেচনায় সরকারি, বেসরকারি ও আর্থিক খাতসহ বিভিন্ন ক্ষেত্রে ক্লাউড কম্পিউটিং ব্যবহারের চাহিদা বৃদ্ধি পাচ্ছে। এছাড়াও দেশে সরকারি ও বেসরকারি পর্যায়ে ইতিমধ্যে ক্লাউড সেবা প্রদানে বিভিন্ন প্রতিষ্ঠান কাজ করছে। আন্তর্জাতিক ক্লাউড সেবা প্রদানকারী বিভিন্ন প্রতিষ্ঠান থেকে সেবা গ্রহণের হার প্রতিনিয়ত বৃদ্ধি পাচ্ছে। ক্লাউড সংক্রান্ত এসকল বিষয়কে সমন্বিত করা, ক্লাউড সেবা প্রদানে মানদন্ড নির্ধারণ, ক্লাউড সেবা গ্রহণের শর্তাবলী, ক্লাউড সেবা ব্যবহারে ঝুঁকি নিরুপন ও তথ্য নিরাপত্তা নিশ্চিতকরণ, হাইব্রিড ক্লাউড ব্যবহারের উপযোগিতা, সরকারি পর্যায়ে আন্তর্জাতিক ক্লাউড সেবাদানকারী হইতে সেবা গ্রহণের ক্ষেত্রসমূহ নির্ধারণ, সরকারি ক্লাউড সেবা প্রদানকারীর সেবাসমূহ বৃদ্ধি ও আন্তর্জাতিক মানসম্পন্নকরণ ইত্যাদি বিষয়সমূহ এই নীতিমালায় অন্তর্ভুক্ত করা হয়েছে।

খসড়া

২. সংক্ষিপ্ত শিরোনাম ও প্রবর্তন:

(ক) এই নীতিমালা 'জাতীয় ডাটা সেন্টার ক্লাউড কম্পিউটিং নীতিমালা ২০২৩' নামে অভিহিত হবে;

(খ) এটি অবিলম্বে কার্যকর হবে।

৩. সংজ্ঞা:

১. **ক্লাউড কম্পিউটিং:** ক্লাউড কম্পিউটিং এর বিভিন্ন ধরণের সংজ্ঞা রয়েছে। ন্যাশনাল ইনস্টিটিউট অফ স্টান্ডার্ডস এন্ড টেকনোলজি (NIST) এর সংজ্ঞা অনুযায়ী বাংলাদেশ সরকার ক্লাউড কম্পিউটিংকে নিম্নরূপে সংজ্ঞায়িত করেছে:

"ক্লাউড কম্পিউটিং হল গ্রাহকের চাহিদা অনুযায়ী নেটওয়ার্কের মাধ্যমে অংশীদারির (shared) ভিত্তিতে কম্পিউটার রিসোর্স যেমন, নেটওয়ার্ক, সার্ভার, স্টোরেজ, এপ্লিকেশন ও ডিজিটাল সেবা ইত্যাদি এর ব্যবহারোপযোগী একটি সামষ্টিক মডেল, যা চাহিদা অনুযায়ী সহজে কনফিগারযোগ্য এবং যা ক্লাউড সেবা প্রদানকারী প্রতিষ্ঠানের সামান্য প্রচেষ্টায় এবং দ্রুততম সময়ে প্রস্তুত ও ব্যবহার করা সম্ভব"।

২. **মাল্টি-টেনান্সি প্লাটফর্ম (Multi Tenancy Platform):** ক্লাউড সেবা প্রদানকারী প্রতিষ্ঠান একই যন্ত্রাদি ব্যবহার করে একাধিক গ্রাহককে সেবা গ্রহনের সুযোগ প্রদান করে থাকে। অবকাঠামোভিত্তিক সেবার (IaaS) ক্ষেত্রে হাইপার ভাইসর (Hyper Visor) প্রযুক্তির মাধ্যমে একই যন্ত্রাদি ব্যবহার করে একাধিক ভার্চুয়াল সার্ভার চালু থাকে। প্লাটফর্মভিত্তিক সেবার (PaaS) ক্ষেত্রে একই অপারেটিং সিস্টেম ও নেটওয়ার্ক ব্যবহার করে গ্রাহকগণ ভিন্ন ভিন্ন সফটওয়্যার ও এপ্লিকেশন ব্যবহার করতে পারেন। সফটওয়্যারভিত্তিক সেবার (SaaS) ক্ষেত্রে বিভিন্ন গ্রাহক একই সফটওয়্যারের সেবা গ্রহণ করে থাকেন।

৩. **চাহিদামত স্ব-পরিবেশন (On-Demand Self-Service):** গ্রাহকরা সেবা সরবরাহকারীর সাহায্য ছাড়াই তথ্য প্রযুক্তি সম্পদ (Resource) যেমন, ভার্চুয়াল সার্ভার বা ইমেইল অ্যাকাউন্ট ইত্যাদি সংস্থান করতে সক্ষম হন।

৪. **বিস্তৃত নেটওয়ার্কে এক্সেস (Broad Network Access):** গ্রাহকরা বিভিন্ন যন্ত্রাদি (উদাঃ স্মার্ট ফোন, ট্যাবলেট, ল্যাপটপ) থেকে সর্বত্র প্রচলিত ক্লায়েন্ট (উদাঃ একটি ওয়েব ব্রাউজার) ব্যবহার করে ইন্টারনেটের মাধ্যমে নেটওয়ার্কে এক্সেস করতে সক্ষম হন।

খসড়া

৫. **তথ্য প্রযুক্তি সম্পদের একত্রীকরণ (Resource Pooling):** সেবা প্রদানকারীর কম্পিউটিং সম্পদসমূহ একাধিক গ্রাহককে ডিজিটাল সেবা আকারে সরবরাহ করার জন্য একত্রিত করা হয়। সাধারণত, ভার্চুয়ালাইজেশন প্রযুক্তির সাহায্যে বহু-প্রজাসত্ত্বের (multi-tenancy) সুবিধার মাধ্যমে কম্পিউটিং সম্পদকে গ্রাহকের চাহিদার প্রেক্ষিতে নির্ধারণ এবং পুনরায় নতুন গ্রাহককে স্থানান্তর করা হয়।

৬. **দ্রুত হ্রাস বৃদ্ধির সুবিধা (Rapid Elasticity):** কম্পিউটিং সম্পদ চাহিদার ভিত্তিতে স্বয়ংক্রিয়ভাবে দ্রুত বন্দোবস্তকরণ ও ব্যবহার শেষে বিমুক্তকরণ। গ্রাহক তার প্রয়োজন অনুসারে সহজেই ক্লাউড সেবার ব্যবহার কম-বেশি করতে পারেন।

৭. **পরিমিত সেবা (Measured Service):** গ্রাহকরা শুধুমাত্র তাদের ব্যবহৃত কম্পিউটার সম্পদের জন্য অর্থ পরিশোধ করবেন। সাধারণত সেবা প্রদানকারী গ্রাহকের ব্যবহার পর্যবেক্ষণের নিমিত্তে গ্রাহককে ড্যাশবোর্ড সরবরাহ করে থাকে।

৮. **ন্যাশনাল ইনস্টিটিউট অফ স্ট্যান্ডার্ডস অ্যান্ড টেকনোলজি (NIST):** NIST হল মার্কিন যুক্তরাষ্ট্রের বাণিজ্য বিভাগের একটি সংস্থা যার লক্ষ্য হল আমেরিকান উদ্ভাবন এবং শিল্প প্রতিযোগিতার প্রচার করা।

৯. **SOC 2 Type II:** SOC 2 Type II হল সিস্টেমে প্রয়োগকৃত অভ্যন্তরীণ কন্ট্রোল ব্যবস্থাপনার প্রতিবেদন যার মাধ্যমে কোম্পানি কীভাবে গ্রাহকের উপাত্ত সংরক্ষন করছে এবং সেই কন্ট্রোলসমূহ কতটা ভালভাবে কাজ করছে তা নির্ণয় করে৷ ক্লাউড পরিষেবা দানকারী কোম্পানিসমুহ তৃতীয় পক্ষ সরবরাহকৃত প্রযুক্তির ঝুঁকি মূল্যায়ন এবং তা কিভাবে মোকাবেলা করা যায় তা নির্ণয় করতে SOC 2 ব্যবহার করে৷

৪. মূলনীতিসমূহ (Principles)

(ক) বাংলাদেশ সরকার ও এর প্রত্যেক মন্ত্রণালয়ের কার্যক্রম, আইন ও আদেশের সাথে সামঞ্জস্য রেখে সর্বজনীন ক্লাউড সেবার অগ্রাধিকার (Cloud First) নীতি প্রবর্তন;

(খ) সরকারি সংস্থায় ক্লাউড প্রযুক্তি প্রবর্তনের মাধ্যমে সেবাসমূহ সর্বজনীন, সহজ ও সৃজনশীল করা;

(গ) ক্লাউড প্রযুক্তির মাধ্যমে অবকাঠামোগত ব্যয় হ্রাস করে কর্মক্ষমতার বৃদ্ধিকরণ ও দ্রুত সংস্থাপন নিশ্চিতকরন;

খসড়া

৫. উদ্দেশ্যসমূহ (Objectives)

(ক) সকল সরকারি প্রতিষ্ঠানে আইটি সংস্থাপনে ক্লাউড কম্পিউটিং এর ব্যবহার নিশ্চিতকরণ;

(খ) ক্লাউড কম্পিউটিং এর নিরাপত্তা নিশ্চিতকরণ;

(গ) ক্লাউড পরিষেবা প্রদানকারী প্রতিষ্ঠান এবং ক্লাউড সেবা গ্রহণকারী সরকারি ও বেসরকারি প্রতিষ্ঠানের দায়িত্বাবলী নির্ধারন;

(ঘ) ক্লাউডে তথ্য নিরাপত্তা ও গোপনীয়তা নিশ্চিতকরণ;

৬. পরিধি (Scope)

(ক) স্থানীয় পর্যায়ে ক্লাউড সেবা প্রদানকারী ও সংশ্লিষ্ট সকল সেবা গ্রহণকারী সরকারি, রাষ্ট্রীয় মালিকানাধীন, বহুজাতিক এবং ব্যক্তিমালিকানাধীন সংস্থার উপর এই নীতি প্রযোজ্য হবে।

(খ) সকল সরকারি সংস্থা সরকারি ক্লাউড ব্যবহার করবে। তথ্য ও যোগাযোগ প্রযুক্তি বিভাগের অধীনস্ত বাংলাদেশ কম্পিউটার কাউন্সিল (বিসিসি) সরকারি ক্লাউড সেবার বাস্তবায়নকারী হিসাবে কাজ করবে।

(গ) এই নীতিমালা বাংলাদেশের সকল সরকারি, আধা-সরকারি, স্বায়ত্বশাসিত, সংবিধিবদ্ধ সংস্থা, রাষ্ট্রায়ত্ব প্রতিষ্ঠান এবং সংস্থার ক্ষেত্রে প্রযোজ্য হবে।

৭. ক্লাউড বিস্তার (Deployment) মডেল

(১) **পাবলিক ক্লাউড (Public Cloud):** এই ক্লাউড অবকাঠামো সর্বসাধারণের ব্যবহারের জন্য উন্মুক্ত। এটি ব্যবসা প্রতিষ্ঠান, শিক্ষা প্রতিষ্ঠান বা সরকারি প্রতিষ্ঠান অথবা এই তিন ধরণের সংস্থার যৌথ মালিকানায় পরিচালিত হতে পারে। এটি ক্লাউড সেবা প্রদানকারীর নিজস্ব স্থাপনায় থাকে।

(২) **প্রাইভেট ক্লাউড (Private Cloud):** এই ক্লাউড অবকাঠামো কেবলমাত্র একটি সংস্থার বিভিন্ন গ্রাহকদের (উদাঃ ব্যবসায়িক ইউনিটসমূহ) ব্যবহারের জন্য তৈরি করা হয়। এটি উক্ত সংস্থা বা তৃতীয় পক্ষ অথবা দুইয়ের যৌথ মালিকানায় পরিচালিত হতে পারে এবং একই স্থাপনায় অথবা দূরবর্তী স্থানে থাকতে পারে।

(৩) **কমিউনিটি ক্লাউড (Community Cloud):** এই ক্লাউড অবকাঠামোটি সংস্থার স্বার্থ সংশ্লিষ্ট (উদাঃ লক্ষ্য, সুরক্ষার বাধ্যবাধকতা, নীতিমালা, এবং এর পরিপালন বিবেচনায়) একটি নির্দিষ্ট ভোক্তাগোষ্ঠীকে

খসড়া

স্বতন্ত্রভাবে ব্যবহারের জন্য প্রদান করা হয়। এটি গোষ্ঠীভুক্ত এক বা একাধিক সংস্থা, তৃতীয় পক্ষ বা এর যৌথ মালিকানায় পরিচালিত হতে পারে এবং একই স্থাপনায় অথবা দূরবর্তী স্থানে থাকতে পারে।

(৪) **হাইব্রিড ক্লাউড (Hybrid Cloud):** তথ্য ও এপ্লিকেশন বিভিন্ন প্লাটফর্মে সঠিকভাবে পরিচালনার নিমিত্তে মানদণ্ড বা বাণিজ্যিক প্রযুক্তি দ্বারা যুক্ত দুই বা ততোধিক স্বতন্ত্র ক্লাউড অবকাঠামোর (পাবলিক, প্রাইভেট অথবা কমিউনিটি) সমন্বয়ে এই ক্লাউড অবকাঠামো গঠিত (যেমন, ভিন্ন ক্লাউডের মধ্যে কার্যভারের ভারসাম্য রক্ষার্থে ব্যবহৃত ক্লাউড বার্স্টিং (Bursting)।

৮. ক্লাউড সেবা (Service) মডেল:

১. **কার্যক্রম প্রক্রিয়া ভিত্তিক সেবা (BPaaS):** ক্লাউড সেবা মডেলের উপর নির্ভর করে গ্রাহককে সেবার সংখ্যা (Horizontal) বা সেবার সক্ষমতা (Vertical) বৃদ্ধি করে কর্মক্রম বিস্তারের ক্ষমতা দেয়া হয়। এই ক্লাউড সেবা অন্যান্য ক্লাউড সেবা যেমন, সফটওয়্যারভিত্তিক সেবা (SaaS), প্লাটফর্মভিত্তিক সেবা (PaaS) এবং অবকাঠামোভিত্তিক সেবা (IaaS) এর উপর নির্ভরশীল।

২. **সফটওয়্যারভিত্তিক সেবা (SaaS):** ক্লাউড সেবা প্রদানকারী ক্লাউডে চলমান এপ্লিকেশনসমূহ গ্রাহকের ব্যবহারের জন্য প্রদান করে থাকে। এই এপ্লিকেশনসমূহ বিভিন্ন থিন ক্লায়েন্ট যেমন, ওয়েব ব্রাউজার অথবা সফটওয়্যার ইন্টারফেসের মাধ্যমে অভিগম্য হয়ে থাকে। ক্লাউড অবকাঠামোর অন্তর্নিহিত নেটওয়ার্ক, সার্ভার, অপারেটিং সিস্টেম, স্টোরেজ অথবা এপ্লিকেশনসমূহের উপর গ্রাহকের কোন নিয়ন্ত্রণ থাকে না, শুধুমাত্র নির্দিষ্ট এপ্লিকেশনের ব্যবহারকারী সীমিত পরিসরে সেবার রূপরেখা (Configuration) পরিবর্তন করতে পারে।

৩. **প্লাটফর্মভিত্তিক সেবা (PaaS):** ক্লাউড সেবা প্রদানকারীর সমর্থিত প্রোগ্রামিং ভাষা, লাইব্রেরী, সেবাসমূহ ও সরঞ্জাম ব্যবহার করে গ্রাহক কর্তৃক নির্মিত বা ক্রয়কৃত এপ্লিকেশনসমূহ সংস্থাপন করার ক্ষমতা গ্রাহককে দেয়া হয়। ক্লাউড অবকাঠামোর অন্তর্নিহিত নেটওয়ার্ক, সার্ভার, অপারেটিং সিস্টেম, স্টোরেজ অথবা এপ্লিকেশনসমূহের উপর গ্রাহকের কোন নিয়ন্ত্রণ থাকে না, তবে সংস্থাপিত এপ্লিকেশন এবং উক্ত এপ্লিকেশন সংস্থাপনের নিমিত্তে প্রয়োজনীয় রূপরেখা পরিবর্তন করতে পারে।

৪. **অবকাঠামোভিত্তিক সেবা (IaaS):** এই সেবার আওতায় গ্রাহককে কম্পিউটিং প্রসেসিং, স্টোরেজ বা তথ্য সংরক্ষণ সিস্টেম, নেটওয়ার্ক, এবং অন্যান্য মৌলিক কম্পিউটিং সুবিধা প্রদান করা হয়, যেখানে গ্রাহক তার সফটওয়্যার চালাতে সক্ষম এবং এতে অপারেটিং সিস্টেম এবং সেবার চুক্তি (SLA) অনুযায়ী এপ্লিকেশন অন্তর্ভুক্ত থাকতে পারে। এই সেবাটিতে গ্রাহক মূল কম্পিউটিং অবকাঠামো পরিচালনা বা নিয়ন্ত্রণ করে না। তবে অপারেটিং সিস্টেম, স্টোরেজ ডিভাইস এবং এপ্লিকেশনসমূহে নিয়ন্ত্রণ থাকে। নির্বাচিত নেটওয়ার্কিং ডিভাইসে যেমন হোস্ট ফায়ারওয়াল সীমিত নিয়ন্ত্রণ থাকে।

খসড়া

৫. **কন্টেইনারভিত্তিক সেবা (CaaS)**: এই সেবার আওতায় গ্রাহককে দ্রুত সফটওয়্যার তৈরিতে স্যান্ডবক্স (Sandbox), প্রয়োজনীয় প্রোগ্রামিং ভাষায় কাজ করার পরিবেশ এবং অন্যান্য সুযোগ সুবিধা প্রদান করা হয়। সফটওয়্যার প্রকৌশলী এবং অন্যান্য আইটি পেশাজীবি পৃথক প্লাটফর্মের ভার্চুয়ালাইজেশন ব্যবহার করে সফটওয়্যার তৈরি, পরীক্ষণ এবং পরীক্ষামূলকভাবে চালু করতে পারেন।

৯. ক্লাউড সেবা প্রদানকারী (সিএসপি) এর দায়িত্বাবলী

ক্লাউড সেবা সরবরাহকারী (সিএসপি) প্রতিষ্ঠান তথ্যের শ্রেণী অনুযায়ী নিম্নোক্ত দায়িত্ব অবশ্যই পালন করবে:

১. **মানদন্ড (Standard):** সিএসপি নিম্নোক্ত মানদন্ড অনুসরন করতে পারে:

ক) ISO/IEC 27017 প্রত্যয়িত এবং অনুমোদিত / আন্তর্জাতিকভাবে গ্রহণযোগ্য মানদন্ড; অথবা

খ) ক্লাউড সিকিউরিটি এলায়েন্স (Cloud Security Alliance) সিকিউরিটি ট্রাস্ট এন্ড এস্যুরেন্স রেজিস্ট্রি (Security Trust and Assurance Registry) এর দ্বিতীয় স্তরের (ব্রোঞ্জঃ Bronze Award) ন্যুনতম প্রত্যয়ন। এই নিমিত্ত সংযুক্তি ‘ক’তে উল্লেখিত ক্লাউড ম্যাচুরিটি ম্যাট্রিক্স (CMM) অনুসরন করতে পারে।

২. **নিরীক্ষণ (Audit)**:

সিএসপিকে স্বাধীন তৃতীয় পক্ষের নিরীক্ষক দ্বারা ক্লাউড নিরাপত্তা মানদন্ডের আলোকে বাৎসরিক ভিত্তিতে SOC 2 Type II নিরীক্ষা সম্পাদন করতে হবে এবং উক্ত নিরীক্ষার বিস্তারিত প্রতিবেদন ডিজিটাল নিরাপত্তা এজেন্সির নিকট দাখিল করতে হবে। সিএসপিকে অবশ্যই সুরক্ষার সকল বাধ্যবাধকতা প্রতিপালন করছে এই মর্মে প্রমাণাদি প্রদর্শন করতে হবে।

৩. **এক্সেস নিয়ন্ত্রণ (Access Control):** সিএসপিকে একটি এক্সেস নিয়ন্ত্রণ নীতি ও পদ্ধতি বাস্তবায়ন করতে হবে যাতে বোর্ডিং, অফ-বোর্ডিং, ব্যবহারের প্রাধিকার পরিবর্তন, নিয়মিত এক্সেস নীতি পর্যালোচনা, প্রশাসকের ক্ষমতা ও এর নিয়ন্ত্রিত ব্যবহার (limit and control use of administrator privileges) এবং কোন ব্যবহারকারীর নিষ্ক্রিয়তার সময়সীমা (Inactivity timeouts) নির্ধারণ করা থাকবে। সিএসপিকে অবশ্যই সাংঘর্ষিক দায়িত্ব ও কর্তব্যসমূহ (যেমন: Separation of Duties) শনাক্ত এবং পৃথক করতে হবে। সুস্পষ্ট, কল্পিত বা অব্যবহৃত অ্যাকাউন্ট শনাক্ত করার জন্য সিএসপিকে অবশ্যই কম্পিউটার অ্যাকাউন্টগুলির বর্তমান এবং সঠিক তালিকা বজায় রাখতে হবে এবং নিয়মিতভাবে

খসড়া

তালিকাটি পর্যালোচনা করতে হবে। সিএসপিকে অবশ্যই লগ-অন প্রচেষ্টা (A limit on logon attempts) সীমিতকরণ, সমবর্তী (Concurrent) সেশনের সংখ্যা নির্ধারণ এবং একাধিক সত্যতা যাচাইকরণ (Multi factor authentication) পদ্ধতি প্রয়োগ করতে হবে। এক্সেস নিয়ন্ত্রণের জন্য কেন্দ্রীয়ভাবে পরিচালিত এক্সেস নিয়ন্ত্রণ প্রটোকল (Access Protocol) ব্যবহার করা আবশ্যক। এই জন্য ইউনিক্স (UNIX) বা লিনাক্স (Linux) সমর্থিত ক্লাউড কম্পিউটিং এর ক্ষেত্রে লাইটওয়েট ডিরেকটরি একসেস প্রটোকল (LDAP) এবং উইন্ডোজ (Windows) সমর্থিত ক্লাউড কম্পিউটিং এর ক্ষেত্রে একটিভ ডিরেক্টরি (AD) ব্যবহার করা আবশ্যক। অবকাঠামোভিত্তিক সেবা (IaaS) এর প্রযোজ্য ক্ষেত্রে ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN) সেবার মাধ্যমে অপারেটিং সিস্টেমে অভিগমনের ব্যবস্থা করতে হবে।

৪. **পাসওয়ার্ডঃ (Password):** সিএসপি পাসওয়ার্ডের দৈর্ঘ্য, জটিলতা ও ইতিহাসের ভিত্তিতে পাসওয়ার্ড ভিত্তিক সত্যতা যাচাই করবে। প্রয়োজনে একাধিক সত্যতা যাচাইকরণ (Multi factor authentication) ও একক সাইন অন (Single Sign On) প্রযুক্তির ব্যবহার নিশ্চিত করবে। সিএসপি ক্লাউড ব্যবহারকারীকে প্রথম লগইনেই পাসওয়ার্ড পরিবর্তন করতে বাধ্য করবে এবং ব্যবহারকারীর সাথে পাসওয়ার্ড সংক্রান্ত সকল যোগাযোগ দাপ্তরিক ইমেইল এর মাধ্যমে হতে হবে।

৫. **সচেনতাঃ (Awareness):** সিএসপি নিজস্ব জনবলের মধ্যে নিরাপত্তা সচেনতা সৃষ্টির লক্ষ্যে নিয়মিত প্রশিক্ষণের ব্যবস্থা করবে। এছাড়াও সিএসপি জনসচেনতা সৃষ্টির উদ্দেশ্যে নিয়মিত একটি পোর্টালে সাইবার ঝুঁকির তালিকা প্রকাশ করবে।

৬. **লগ সংরক্ষণঃ (Log Storage):** সিএসপি প্রতিষ্ঠানের সংরক্ষন নীতিমালা অনুযায়ী লগ সংরক্ষণ করবে এবং সংরক্ষন শেষে নীতিমালা অনুযায়ী নিরাপদে মুছে ফেলতে ব্যবস্থা গ্রহণ করবে। অনলাইনে লগ দেখবার জন্য সিএসপি গ্রাফিক্যাল ইউজার ইন্টারফেস (GUI) প্রদান করবে। সিএসপি ডিজিটাল নিরাপত্তা এজেন্সিকে লগ প্রেরণের ব্যবস্থা করবে। এছাড়াও সিএসপিকে নিজস্ব লগ নিরীক্ষণ ও সেই অনুযায়ী প্রয়োজনীয় সতর্কতা জারি করার জন্য প্রযুক্তিগত সক্ষমতা থাকতে হবে।

৭. **তদন্তঃ (Investigation):** সিএসপি যেকোন নিরাপত্তা সংক্রান্ত তদন্ত রিপোর্ট তদন্ত সম্পন্ন হওয়ার পরবর্তী ২ বৎসর পর্যন্ত সংরক্ষণ করবে। সিএসপি নিরাপত্তা সংক্রান্ত তদন্ত কাজে ডিজিটাল নিরাপত্তা এজেন্সি এবং অন্যান্য আইন প্রয়োগকারী সংস্থাকে প্রয়োজনীয় সহায়তা করবে।

৮. **সময়ের সমন্বয় (Synchronization of Time):** সিএসপিকে নির্দিষ্ট মান অনুযায়ী এর সকল সার্ভারের ঘড়ির সময় জাতীয় টাইম সার্ভার এর সাথে সমলয়িত (Synchronized) রাখতে হবে।

৯. **পরিবর্তন নিয়ন্ত্রণঃ (Change Control):** ক্লাউড কম্পিউটিং প্লাটফর্মের যেকোন পরিবর্তনের ক্ষেত্রে প্রয়োজনীয় নিয়ন্ত্রণ প্রতিষ্ঠার জন্য সিএসপি সর্বজনস্বীকৃত পদ্ধতি অবলম্বন করবে। যেকোন পরিবর্তন প্রোডাকশন পরিবেশে প্রয়োগের পূর্বে তা পরীক্ষামূলক ভাবে ব্যবহার করতে হবে। সিএসপি পরীক্ষা পরিচালনার সময় মূল তথ্য ব্যবহার করবে না।

১০. **কনফিগারেশন / প্যাচ ব্যবস্থাপনা (Configuration/Patch Management):** সিএসপি এর তথ্য সুরক্ষা সংক্রান্ত নীতিমালা থাকতে হবে। যথাযথ মানদন্ড অনুযায়ী সিএসপি এর সিস্টেম এবং সার্ভারসমূহের নিরাপত্তা নিশ্চিত করিবে এবং ডাটাবেসের সুরক্ষার নিমিত্তে প্রত্যেক ডাটাবেসকে লজিক্যালি পৃথক করবে এবং এনক্রিপ্ট করবে। সিএসপি ক্লাউড ব্যবস্থাপনায় ব্যবহৃত কম্পিউটারসমূহের প্যাচ (Patch) হালনাগাদ করবে এবং লাইসেন্সড অ্যান্টিভাইরাস দ্বারা সুরক্ষিত রাখবে। সিএসপি ভৌত নিরাপত্তা (Physical Security) ব্যবস্থা জোরদার করবে। যথাযথ মানদন্ড অনুযায়ী প্রোগ্রামিং ইন্টারফেস ব্যবহার করে সফটওয়্যার তৈরি করবে।

১১. **বিসিপি/ ডিআরপি (BCP/DRP):** সিএসপি সেবার নিরবিচ্ছিন্নতা প্রতিষ্ঠা এবং দুর্যোগ পরবর্তী পুনরুদ্ধার পরিকল্পনা অনুসরণ করবে যা প্রতি বছর পরীক্ষা ও পূনঃমূল্যায়ন করা হবে। দুর্যোগ পরবর্তী পুনরুদ্ধার পরিকল্পনা অনুসারে সিএসপি নিয়মিত ব্যাকআপ গ্রহন ও সংরক্ষন করবে। এছাড়াও সিএসপি এর সংঘটিত ঘটনার প্রতিক্রিয়া পরিকল্পনা থাকবে যা প্রতি বছর পরীক্ষা ও পূনঃমূল্যায়ন করা হবে। ডাটা সেন্টার নির্দেশিকা ২০২০ অনুযায়ী তথ্য প্রযুক্তি সেবার নিরবিচ্ছিন্নতা প্রতিষ্ঠা করতে এবং বজায় রাখতে ISO 22301 এবং দুর্যোগ পরবর্তী তথ্য পুনরুদ্ধারে ISO 24762 মানদন্ড অনুসরণ করতে হবে। এছাড়াও বছরে ন্যুনতম একবার সেবার নিরবিচ্ছিন্নতা পরীক্ষা করা আবশ্যক।

১২. **মালামাল হস্তান্তর (Asset Disposal):** তথ্যের নিরাপত্তা ও গোপনীয়তা রক্ষা এবং পরিবেশের দূষণরোধ নিশ্চিতকরন পূর্বক হার্ডওয়্যার সংক্রান্ত মালামাল হস্তান্তরের ব্যবস্থা গ্রহন করবে।

খসড়া

১৩. হুমকি / ঝুঁকির মূল্যায়নঃ (Evaluation of Risk): সিএসপি অবশ্যই নতুন সিস্টেম অথবা বিদ্যমান সিস্টেমে কোন পরিবর্তনের আগে হুমকি এবং ঝুঁকি মুল্যায়ন করিবে। এই জন্য জাতীয় ডাটা সেন্টার নির্দেশিকায় উল্লেখিত নিয়মতান্ত্রিক, প্রক্রিয়া ভিত্তিক ঝুঁকি ব্যবস্থাপনার জন্য BDS 27005 মানদন্ড মেনে চলতে হবে।

যেহেতু বাংলাদেশ সরকার কর্তৃক গৃহীত ক্লাউড সুরক্ষার মানদন্ড প্রতিপালন প্রয়োজনীয় নিরাপত্তা নিয়ন্ত্রণের অবিচ্ছেদ্য অংশ, সেহেতু একজন বহিরাগত নিরীক্ষক দ্বারা ঝুঁকি মূল্যায়ন করাতে হবে এবং প্রয়োগযোগ্য ক্ষেত্রে সিএসপির বিবৃতি ও বহিরাগত নিরীক্ষকের হালনাগাদ প্রতিবেদনের মূল্যায়নই যথেষ্ট বলে বিবেচিত হবে।

১৪. দুর্বলতা মূল্যায়ন (Vulnerability Assessment): সিএসপি অবশ্যই নতুন সিস্টেম অথবা বিদ্যমান সিস্টেমের নিরাপত্তার দুর্বলতা অনুসন্ধান ও মুল্যায়নের জন্য Vulnerability Test এবং Penetration Test প্রতি বছর অন্তত একবার পরিচালনা করবে। সকল সফটওয়্যার এবং সিস্টেম এই নিরাপত্তা পরীক্ষার আওতাধীন হবে।

১৫. নিরাপত্তা স্ক্রিনিং: সিএসপি তথ্য সিস্টেমে এক্সেস অনুমোদনের আগে ব্যক্তিদের অতীত কর্মকান্ডের ইতিহাস (Background) পরীক্ষা করবে। বিশেষতঃ সিএসপি এর কর্মীদের ফৌজদারী নথি বিবেচনা পূর্বক নিয়োগ দান করবে।

১৬. সরবরাহ চেইনঃ (Supply Chain): সিএসপি এর সরবরাহকারী এবং ঠিকাদারদের সুরক্ষা নীতি যেন সিএসপির নিজস্ব সুরক্ষা নীতিগুলি পূরণ বা অতিক্রম করে তা নিশ্চিত করবে।

১৭. এনক্রিপশন (Encryption): সিএসপি অবশ্যই সরকারি তথ্য আদান প্রদান ও সংরক্ষণের সময় তথ্য ভালোভাবে এনক্রিপ্ট করবে এবং এনক্রিপশন কী (Key) প্রযুক্তি পরিচালনায় দক্ষ হবে।

১৮. লজিক্যাল বিভক্তি (Logical Segregation): সিএসপি রাষ্ট্রীয় তথ্য লজিক্যালি আলাদা রাখিবে এবং রাষ্ট্রীয় তথ্য প্রবাহ অন্যান্য গ্রাহক ও সিস্টেম পরিচালনা তথ্য প্রবাহ থেকে আলাদা রাখবে। এই উদ্দেশ্যে সিএসপি নিরাপত্তা যন্ত্রাংশ ব্যবহার করবে।

খসড়া

১৯. প্রযুক্তিগত নিয়ন্ত্রণ (Technological Control): সিএসপিকে ফায়ারওয়াল এবং অবৈধ বা অযাচিত অনুপ্রবেশ প্রতিরোধ ব্যবস্থা বাস্তবায়ন করতে হবে। সিএসপিকে অ্যাপ্লিকেশন স্তরে ফায়ারওয়াল প্রয়োগ করতে হবে। সিএসপি অবকাঠামো সেবার (IaaS) গ্রাহককে ফায়ারওয়াল, অনুপ্রবেশ প্রতিরোধ, অ্যান্টিভাইরাস এবং এনক্রিপশন হিসাবে সুরক্ষা ব্যবস্থার রূপরেখা সম্পর্কে অবহিত করবে। যথাযথ মানদন্ড অনুযায়ী সিএসপি দূরবর্তী এক্সেস ব্যবস্থা সুরক্ষিত করবে। সিএসপি সেবা বিতরনের ব্যত্যয়ের বিস্তৃত আক্রমন (Distributed Denial of Service: DDoS) হতে সুরক্ষার ব্যবস্থা করবে।

২০. নিরাপত্তা লংঘন (Security Incident) অবহিতকরণঃ রাষ্ট্রীয় তথ্যকে প্রভাবিত করতে পারে এমন প্রকৃত অথবা সম্ভাব্য নিরাপত্তার লংঘনের ঘটনা ২৪ ঘন্টার মধ্যে রাষ্ট্রকে অবহিত করবে। সুরক্ষা নীতি, পদ্ধতি অথবা চুক্তিতে কোন পরিবর্তন হলে রাষ্ট্রকে ২৪ ঘন্টার মধ্যে অবহিত করবে।

২১. Proprietary সফটওয়্যার ব্যবহারঃ অবকাঠামোভিত্তিক সেবা (IaaS) এর প্রযোজ্য ক্ষেত্রে লাইসেন্সবিহীন, চুরিকৃত (Pirated) এবং লাইসেন্সের মেয়াদোত্তীর্ণ সফটওয়্যার ব্যবহার করা যাবে না। মুক্ত সফটওয়্যার (Open Source), উন্মুক্ত কোড লাইব্রেরী ব্যবহার করে নির্মিত সফটওয়্যার, বিনামূল্যের সফটওয়্যার (Freemium) এবং কাস্টমাইজড (Customized) সফটওয়্যারসমূহ ব্যবহারের ক্ষেত্রে বাংলাদেশ কম্পিউটার কাউন্সিলের সফটওয়্যার এবং হার্ডওয়্যারের গুণগত মান পরীক্ষাকরণ ও সার্টিফিকেশন সেন্টার হতে প্রয়োজনীয় নিরাপত্তার ও কার্যকারিতার প্রত্যয়ন গ্রহণ করা বাধ্যতামূলক। এছাড়াও কাস্টমাইজড (Customized) সফটওয়্যারসমূহের জন্য ISO 9001 প্রত্যয়নের উপর গুরুত্বারপ করা হল।

২২. ডাটা সেন্টার এবং এর পরিচালনা

(ক) প্রায়শই ক্লাউড সেবার ধরণের কারণে তথ্য সংরক্ষণ ও প্রক্রিয়াকরণের সঠিক অবস্থান এবং নিয়ন্ত্রণ নিয়ে উদ্বেগ দেখা দেয়। ক্লাউড কম্পিউটিং সংক্রান্ত প্রধান উদ্বেগের বিষয় হল সিএসপি দ্বারা গ্রাহকের তথ্য পরিচালনার ধরণ।

(খ) (১)সরকারি সিএসপি পরিচালনাকারী ডাটা সেন্টারে তথ্য ও যোগাযোগ প্রযুক্তি জ্ঞান সম্পন্ন স্থায়ী জনবল থাকতে হবে

(২) বহুজাতিক সিএসপি পরিচালনাকারী ডাটা সেন্টারে অবশ্যই বাংলাদেশী নাগরিকদের অগ্রাধিকার ভিত্তিতে নিয়োগ দিতে হবে

খসড়া

(গ) সরবরাহকারী ও ঠিকাদার সিএসপির ক্লাউড অবকাঠামোর (ডাটা সেন্টার) বর্তমান অথবা ভবিষ্যৎ অবস্থান এবং ক্লাউড পরিচালনার অবস্থান এবং এই অবস্থান পরিবর্তনের তথ্য অন্যকে জানাবে না। তথ্য অপ্রকাশ সম্পর্কিত চুক্তিতে (Non Disclosure Agreement: NDA) আইনীভাবে বিবেচিত ব্যক্তিসমূহ যারা ডাটা সেন্টার ও এর পরিচালনা কেন্দ্রের মালিকানা, পরিচালনা অথবা নিয়ন্ত্রণের সাথে জড়িত যেমন, সরবরাহকারী, ঠিকাদার ও তাদের উপ-ঠিকাদারগণ অন্তর্ভুক্ত থাকবে।

(ঘ) সিএসপি অবশ্যই এর ডাটা সেন্টার, ক্লাউড অবকাঠামো অথবা পরিচালন কেন্দ্রের অবস্থান পরিবর্তনের নিরাপত্তা ঝুঁকি, তা প্রতিরোধে গৃহীত ব্যবস্থাদি এবং অন্যান্য সম্পর্কিত বিষয়াদি গ্রাহককে অবহিত করবে এবং গ্রাহকের অনুমতি পূর্বক উক্ত অবস্থান পরিবর্তন সম্পাদন করবে।

(ঙ) গ্রাহক কোন কারণ প্রদর্শন না করে সিএসপির সাথে পুর্বের চুক্তি বাতিল করতে পারবে। এই কারণে গ্রাহক সতর্কতা অবলম্বন করবে- বিশেষতঃ চুক্তি বাতিলের জন্য প্রয়োজনীয় সময় গ্রহণ; পূর্বের সিএসপির কাছ থেকে প্রয়োজনীয় সহয়তা গ্রহণ এবং প্রয়োজনে বর্তমানে ব্যবহৃত সেবা চালু রাখা- যাতে গ্রাহক তার কার্যক্রম, সেবাসমূহ ও সুরক্ষিত তথ্য-উপাত্ত নতুন সিএসপিতে স্থানান্তর করতে পারে। এছাড়াও এক্ষেত্রে গ্রাহক তার কার্যক্রম, সেবা ও সুরক্ষিত তথ্য-উপাত্তের পরিমান, সংখ্যা ও ঝুঁকির মাত্রা বিবেচনায় নিবে।

১০. সরকারি পর্যায়ে ক্লাউড সেবা গ্রহণকারীর দায়িত্বাবলী

(ক) সরকারি পর্যায়ে ক্লাউড সেবা সরকারি ক্লাউড সেবা প্রদানকারী প্রতিষ্ঠানের নিকট হতে গ্রহণ করা;

(খ) সরকারি ক্লাউড সেবা প্রদানকারী প্রতিষ্ঠান ব্যতীত অন্য কোন বিকল্প ক্লাউড সেবা ব্যবহারের প্রয়োজন হলে বাংলাদেশ কম্পিউটার কাউন্সিলের পরামর্শ ও পূর্বানুমোদন গ্রহণ করা;

(গ) ক্লাউড সেবা গ্রহণের পর চুক্তি অনুযায়ী নিয়মিত মূল্য পরিশোধ করা;

(ঘ) ক্লাউড সেবায় কাস্টমাইজড (Customized) সফটওয়্যারসমূহ ব্যবহারের ক্ষেত্রে বাংলাদেশ কম্পিউটার কাউন্সিলের সফটওয়্যার এবং হার্ডওয়্যারের গুণগত মান পরীক্ষাকরণ ও সার্টিফিকেশন সেন্টার (SQTC) হতে প্রয়োজনীয় নিরাপত্তার ও কার্যকারিতার প্রত্যয়ন গ্রহণ করা;

(ঙ) অবকাঠামোভিত্তিক সেবার (IaaS) ক্ষেত্রে বাংলাদেশ কম্পিউটার কাউন্সিলের বিজিডি ই-গভ সার্ট অনুবিভাগ হতে সিস্টেমের বিদ্যমান নিরাপত্তার দুর্বলতা অনুসন্ধান ও মুল্যায়নের জন্য Vulnerability

খসড়া

Assessment এবং Penetration Test (VAPT) করা এবং প্রতি বছর অন্তত একবার এই কার্যক্রম পরিচালনা করা এবং প্রাপ্ত প্রতিবেদন অনুযায়ী নিরাপত্তার দুর্বলতাসমূহ নির্মূল (Mitigate) করা।

১১. বেসরকারি পর্যায়ে ক্লাউড সেবা গ্রহণকারীর দায়িত্বাবলী:

(ক) বাংলাদেশ সরকারের কোন তথ্য অথবা বাংলাদেশের নাগরিকের কোন ব্যক্তিগত বা আর্থিক তথ্যাদি যেন দেশের ভৌগলিক সীমার বাইরে সংরক্ষণ না করা হয় তা নিশ্চিত করা;

(খ) বিশেষ প্রয়োজনে নাগরিকের তথ্যাদি দেশের ভৌগলিক সীমার বাইরে সংরক্ষণের প্রয়োজন হলে বাংলাদেশ কম্পিউটার কাউন্সিলের পরামর্শ ও পূর্বানুমোদন গ্রহণ করা;

(গ) তথ্য ব্যাক-আপ এবং পুনরুদ্ধারের উদ্দেশ্যে তথ্য দেশের ভৌগলিক সীমার বাইরে সংরক্ষণের প্রয়োজন হলে বাংলাদেশ কম্পিউটার কাউন্সিলের পরামর্শ ও পূর্বানুমোদন গ্রহণ করা;

১২. ক্লাউড সেবার নিরাপত্তা:

(ক) সরকারি ক্লাউডে সরকারি কার্যক্রম এবং তথ্য সংরক্ষণ করলে তথ্য সুরক্ষা বৃদ্ধি পাবে। সরকারি ক্লাউড সেবা প্রদানকারী প্রতিষ্ঠানসমূহকে আন্তর্জাতিক নিরাপত্তার মান এবং যথাযথ প্রত্যয়নপত্র নিশ্চিত করতে হবে। তাদের নিম্নোক্ত প্রাসঙ্গিক শিল্পের মানদণ্ড (Industrial Standard) মেনে চলতে হবে, উদাহরণস্বরূপ,

(১) আন্তর্জাতিক সুরক্ষা মানদণ্ড যেমন আইএসও ২৭০০১: ২০১৩ (যা বিডিএস ২৭০০১:২০১৫ হিসাবে বাংলাদেশ স্ট্যান্ডার্ডস অ্যান্ড টেস্টিং ইনস্টিটিউট গ্রহণ করেছে);

(২) আইটি নিরীক্ষা প্রতিবেদনের জন্য SOC 2 Type I এবং SOC 2 Type II;

(৩) ক্লাউড সিকিউরিটি অ্যালায়েন্স (CSA) এর সিকিউরিটি ট্রাস্ট এন্ড এস্যুরেন্স রেজিস্ট্রি (Security Trust and Assurance Registry) প্রত্যয়ন এবং নিরীক্ষা;

(৪) সেবার ধরণ অনুযায়ী প্রত্যয়ন যেমন পেমেন্ট কার্ড ইন্ডাস্ট্রি ডেটা সিকিউরিটি স্ট্যান্ডার্ড (PCI DSS);

(৫) জাতীয় ডাটা সেন্টার নির্দেশিকা, ২০২০ তে উল্লেখিত অন্যান্য মানদন্ডসমূহ;

(খ) সরকারি সংস্থাসমূহ বাংলাদেশের তথ্য সুরক্ষার জন্য চুক্তিবদ্ধ সেবা প্রদানকারী প্রতিষ্ঠানের সহায়তায় তথ্য সুরক্ষার ব্যবস্থা করবে। এই সুরক্ষা ব্যবস্থায় সংস্থার প্রয়োজনীয়তা অনুযায়ী আন্তর্জাতিক মান ও প্রত্যয়নের সাথে সামঞ্জস্য রেখে ঝুঁকি ব্যবস্থাপনার পদ্ধতি প্রয়োগ করবে। তথ্য নিরাপত্তার ঝুঁকি মুল্যায়নের ভিত্তিতে ক্লাউড সেবার তথ্য সুরক্ষার স্তর চুক্তিতে উল্লেখ করতে হবে। চুক্তিতে প্রয়োজন অনুযায়ী নিম্নোক্ত এক বা একাধিক সুরক্ষা নিয়ন্ত্রক অন্তর্ভুক্ত করা বাঞ্চনীয়।

(১) ভৌত এবং পরিবেশগত নিরাপত্তা;

(২) সেবার নিরবিচ্ছিন্নতা প্রতিষ্ঠা এবং সংঘটিত ঘটনার প্রতিক্রিয়া;

(৩) তালিকাভুক্ত মালামাল এবং উক্ত মালামালের আপেক্ষিক অবস্থান ব্যবস্থাপনা;

(৪) তথ্য এনক্রিপশন (কোনও ক্লাউড সেবা সরবরাহকারীর নিকট সঞ্চিত তথ্য যদি এনক্রিপ্ট করতে হয় তবে এটি সরকারি সংস্থার মালিকানাধীন এবং পরিচালিত ক্রিপ্টোগ্রাফিক কি (key) দ্বারা করতে হবে);

(৫) এক্সেস নিয়ন্ত্রণ, পর্যবেক্ষণ এবং নিবন্ধন;

(৬) নেটওয়ার্ক সুরক্ষা পর্যবেক্ষণ;

(৭) ক্লাউড অ্যাপ্লিকেশানসমূহের মান বাংলাদেশ কম্পিউটার কাউন্সিলের সফটওয়্যার এবং হার্ডওয়্যারের গুণগত মান পরীক্ষাকরণ ও সার্টিফিকেশন সেন্টার (SQTC) কর্তৃক যাচাইকরন এবং প্রত্যয়ন;

(৮) ক্লাউডে সংরক্ষিত তথ্যাদি ব্যবহারকারীর শ্রেণীবিন্যাস অনুসারে তথ্যের এক্সেস নিশ্চিতকরন (Cloud Zoning);

১৩. তথ্য নিরাপত্তা ও গোপণীয়তা:

(ক) গ্রাহকের দায়িত্বাবলীঃ

(১) ক্লাউড কম্পিউটিং এর সাথে সংশ্লিষ্ট সকল কর্মচারী (যেমন প্রয়োগকারী, পরিচালনাকারী এবং রক্ষনাবেক্ষনকারী) আইটি নিরাপত্তা বিষয়ে সচেতনতা বৃদ্ধি করতে হবে।

(২) ক্ষতিকর কোড হতে সুরক্ষা, অ্যান্টি-ভাইরাস সফটওয়্যার এর ব্যবহার বৃদ্ধি, নেটওয়ার্ক এবং সংশ্লিষ্ট অ্যাপ্লিকেশান এর ধারাবাহিক তদারকি নিশ্চিত করতে হবে। এজন্য বাংলাদেশ কম্পিউটার কাউন্সিলের সফটওয়্যার এবং হার্ডওয়্যারের গুণগত মান পরীক্ষাকরণ ও সার্টিফিকেশন সেন্টারের (SQTC) সাহায্য গ্রহণে পরামর্শ দেয়া হচ্ছে।

(৩) এক্সেস নিয়ন্ত্রণ, পর্যবেক্ষণ এবং নিবন্ধন এসএলএ (Service Level Agreement) ও সমঝোতার মাধ্যমে নিশ্চিত করতে হবে।

(খ) ক্লাউড সার্ভিস প্রদানকারীর আইটি নিরাপত্তা বিষয়ক দায়িত্বাবলীঃ

(১) নিরাপত্তা বিষয়ক ফাংশনসমুহকে পৃথকীকরণ এবং ক্লাউড প্লাটফর্মে অগ্রাধিকার নিশ্চিতকরণ।

(২) অ্যাপ্লিকেশান এর বাউন্ডারি সুরক্ষা নিশ্চিতকরণ।

(৩) অ্যাপ্লিকেশান বিভাজিকরন এবং অবকাঠামোর তথ্য সুরক্ষা নিশ্চিতকরণ।

(৪) অননুমোদিত পরিবর্তন রহিতকরনের জন্য সর্বদা তদারকি নিশ্চিতকরন।

(৫) নিয়মিত নিরীক্ষা কার্যক্রম (Regular IT Audit) নিশ্চিতকরন।

(৬) তথ্য ব্যাকআপ এবং পুনরুদ্ধারের জন্য নিয়মিত টেস্টিং এবং ড্রিল সম্পন্নকরন।

(৭) পারিপার্শ্বিক নিয়ন্ত্রণ (Environmental Control) সুনিশ্চিতকরন।

(৮) বাহ্যিক এক্সেস (Physical Access) নিশ্চিতকরণ।

(গ) গ্রাহক ও সেবা প্রদানকারীর মধ্যে বন্টিত দায়িত্বাবলীঃ

(১) ডাটা, সিস্টেম, সার্ভার এবং পারিপার্শ্বিকতার (Environmental) এক্সেস নিয়ন্ত্রণ নিশ্চিতকরণ।

(২) Incident Response এবং রিপোর্টিং নিশ্চিতকরণ।

(৩) ব্যক্তিগত সুরক্ষা নিশ্চিতকরন।

(৪) দৈব দুর্ঘটনার ফলে সৃষ্ট ক্ষতি হ্রাসের পরিকল্পনা সুনিশ্চিত করা।

(ঘ) গ্রাহকের বিজিনেস ব্যবস্থাপকের দায়িত্বাবলীঃ

(১) অভ্যন্তরীণ অথবা বহিঃস্থ সংস্থা দ্বারা নিয়মিত ঝুঁকি মূল্যায়ন এবং হালাগাদকরন নিশ্চিতকরণ।

(২) স্টাফ, প্রয়োজনীয় ফান্ডিং এবং অন্যান্য সুবিধাদি সুনিশ্চিতকরন।

(ঙ) গ্রাহকের আইটি ব্যবস্থাপকের দায়িত্বাবলীঃ

(১) অভ্যন্তরীণ এক্সেস নিয়ন্ত্রণ নীতিমালা ও কার্যপ্রণালীর প্রয়োগ নিশ্চিতকরণ।

(২) সিএসপি -এর দেওয়া একাউন্ট যথাযথ রক্ষণাবেক্ষণ।

(৩) নিয়মিত আইটি নিরাপত্তা সচেতনতা এবং প্রশিক্ষন প্রদান।

(৪) প্রয়োজনীয় বিভিন্ন নীতিমালা এবং কার্যপ্রণালী (আইটি নিরাপত্তা নীতিমালা, দৈব দুর্ঘটনা প্রতিরক্ষা নীতিমালা, কনফিগারেশান ব্যবস্থাপনা নীতিমালা, ভেন্ডর ব্যবস্থাপনা নীতিমালা, সিস্টেম এবং যোগাযোগ ব্যবস্থাপনা নীতিমালা, ঝুঁকি মূল্যায়ন নীতিমালা, সেবা অধিগ্রহণ নীতিমালা ইত্যাদি)

(চ) বহিঃস্থ নিরীক্ষকের দায়িত্বাবলী:

(১) তথ্য নিরাপত্তা মূল্যায়ন এবং প্রতিবেদন প্রদান;

(২) ঝুঁকি মূল্যায়ন (Risk Assessment) এবং প্রতিবেদন প্রদান;

(৩) ক্লাউড ম্যাচুরিটি ম্যাট্রিক্স (CMM) অনুযায়ী মূল্যায়ন ও প্রতিবেদন প্রদান;

(৪) নিরাপত্তা প্রত্যয়ন প্রদান।

১৪. আন্তর্জাতিক পাবলিক ক্লাউড ব্যবহারের পদ্ধতি:

(ক) স্পর্শকাতর এবং গুরুত্বপূর্ণ সরকারি তথ্যাদি যেমন জনগনের ব্যক্তিগত, আর্থিক, স্বাস্থ্য ইত্যাদি সম্পর্কিত তথ্য, সরকারি আর্থিক তথ্যাদি, দেশের নিরাপত্তা সংশ্লিষ্ট তথ্যাদি ইত্যাদি আন্তর্জাতিক পাবলিক ক্লাউডে সংরক্ষন না করা;

(খ) কোন বিশেষ প্রয়োজনে যদি এজাতীয় তথ্য আন্তর্জাতিক পাবলিক ক্লাউডে সংরক্ষন করতে হয়, তাহলে বাংলাদেশ কম্পিউটার কাউন্সিল (বিসিসি) কর্তৃক অবশ্যই অনুমতি গ্রহন করা;

(গ) যদি কোন পাবলিক ক্লাউড সেবা প্রদানকারী প্রতিষ্ঠানের ডাটা সেন্টার বাংলাদেশের ভুখন্ডে স্থাপিত থাকে এবং তথ্যাদি দেশের ভৌগলিক সীমানার মধ্যে থাকবে এই মর্মে নিশ্চয়তা প্রদান করে, কেবল সেক্ষেত্রে সরকারি সংবেদনশীল ও গুরুত্বপূর্ণ তথ্য ঐ সকল আন্তর্জাতিক পাবলিক ক্লাউডে সংরক্ষন করার জন্য বাংলাদেশ কম্পিউটার কাউন্সিল (বিসিসি) বিশেষ বিবেচনায় অনুমোদন প্রদান করতে পারে।

১৫. বাংলাদেশে কার্যক্রম পরিচালনায় আন্তর্জাতিক পাবলিক ক্লাউড সেবাপ্রদানকারীকে প্রদত্ত সুবিধাসমূহ:

(ক) আন্তর্জাতিক পাবলিক ক্লাউড সেবা প্রদানকারীকে তাদের ডাটা সেন্টার বাংলাদেশের ভুখন্ডে স্থাপনের জন্য প্রয়োজনীয় রসদ (যেমনঃ ভুমি, বিদ্যুৎ, মানবসম্পদ ইত্যাদি) ব্যবহারের জন্য প্রয়োজনীয় নিয়মনীতি পালন সাপেক্ষে বাংলাদেশ সরকার অনুমতি প্রদান করতে পারে।

(খ) আন্তর্জাতিক পাবলিক ক্লাউড সেবা প্রদানকারী ওয়ান স্টপ সার্ভিস আইন ২০১৮ এবং ওয়ান স্টপ সার্ভিস (বাংলাদেশ হাইটেক পার্ক কর্তৃপক্ষ) বিধিমালা, ২০১৯ অনুযায়ী হাইটেক পার্কে বিনিয়োগ করতে পারবে।

(গ) আন্তর্জাতিক পাবলিক ক্লাউড সেবা প্রদানকারী প্রতিষ্ঠানের ডাটা সেন্টার স্থাপন ও পরিচালনায় দেশীয় দক্ষ মানব সম্পদকে অগ্রাধিকার প্রদান করা।

১৬. দেশীয় ও আন্তর্জাতিক সহযোগিতা কার্যক্রম:

বাংলাদেশ কম্পিউটার কাউন্সিল ক্লাউড সেবা কার্যক্রম পরিচালনায় সহযোগিতার লক্ষ্যে দেশীয় ও আন্তর্জাতিক পরিমন্ডলে সমপর্যায়ের অথবা সমশ্রেণির বিভিন্ন প্রতিষ্ঠান, সংগঠন, এক্রেডিটেশন বডি, এসোসিয়েশন ইত্যাদির সঙ্গে সমঝোতা স্মারক, দ্বি-পাক্ষিক চুক্তি অথবা সদস্যপদ গ্রহণ করতে পারবে। ক্লাউড কম্পিউটিং সম্পর্কিত নতুন ও টেকসই প্রযুক্তির বিষয়ে জ্ঞান অর্জন, বিতরণের লক্ষ্যে সময় সময় বাংলাদেশ কম্পিউটার কাউন্সিল দেশে বিভিন্ন পর্যায়ে সেমিনার, কর্মশালা, প্রশিক্ষণ ও প্রদর্শনী আয়োজন করবে।

খসড়া

List of Acronyms:

Acronym	Full Name
BDS	Bangladesh Standard
BPaaS	Business Process as a Service
CaaS	Container as a Service
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMM	Cloud Maturity Matrix
COBIT	Control Objectives For Information And Related Technologies
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CTI	Cyber Threat Intelligence
CTO	Chief Technology Officer
DLP	Data Level Parallelism
DMZ	Demilitarized Zone
DR	Disaster Recovery
DSS	Data Security Standard
EMI	Electromagnetic Interference
IaaS	Infrastructure as a Service
ICTDR	ICT Disaster Recovery
IDS	Integrated Data Store
IEC	International Electrotechnical Commission

খসড়া

IOPS	Input/Output Operations Per Second
IP	Internet Protocol
ISACA	Information Systems Audit And Control Association
ISMS	Information Security Management System
ISO	International Standardization Organization
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
LEED	Leadership In Energy And Environmental Design
LT	Linear Technology
MMSB	Multiple Message Switch Buffer
NDA	Non Disclosure Agreement
NIST	National Institute of Standard and Technology
PaaS	Platform as a Service
PCI	Payment Card Industry
PDUs	Power Distribution Units
PVLAN	Private VLAN
RAF	Risk Assessment Framework
SaaS	Software as a Service
SIEM	Security Information And Event Management
SLA	Service-Level Agreement
SPOF	Single Point Of Failure

খসড়া

শব্দকোষ (Glossary):

ক্রম	শব্দ/বিষয়	সংজ্ঞা
১	(Single Point of Failure) ব্যর্থতার একক বিন্দু	ব্যর্থতার একক বিন্দু (SPoF) একটি সিস্টেমের এমন একটি অংশ, যদি এটি ব্যর্থ হয় তবে সমস্ত সিস্টেমটি অচল হয়ে পড়ে। যেসব সিস্টেমে উচ্চ প্রাপ্যতা ও নির্ভরযোগ্যতা দরকার, সেখানে এটা অনাকাঙ্ক্ষিত।
২	প্রাপ্যতা (Availability)	অপারেশানের সময় একটি সিস্টেম, সাবসিস্টেম ও সরঞ্জামাদি চালু রাখার সম্ভাব্যতা।
৩	তথ্য নিরাপত্তা ব্যবস্থাপনা প্রক্রিয়া (ISMS)	তথ্য নিরাপত্তা ব্যবস্থাপনা প্রক্রিয়া হল হুমকি ও দুর্বলতা থেকে সম্পদের গোপনীয়তা, অখন্ডতা ও সহজলভ্যতা নিশ্চিতের জন্য কোন সংস্থাকে যেসব নীতিমালা বাস্তবায়ন করা দরকার, এমন নীতিমালা ও নির্দেশনা বর্ণনা করে।
৪	ক্লাউড কম্পিউটিং (Cloud Computing)	ক্লাউড কম্পিউটিং (Cloud Computing) হল কম্পিউটার রিসোর্স যেমন কম্পিউটার হার্ডওয়্যার, সফটওয়্যার ও নেটওয়ার্ক ডিভাইস ব্যবহার করে কোন সার্ভিস বা সেবা প্রদান করা। ক্লাউড কোন নির্দিষ্ট প্রযুক্তি নয়, বেশ কয়েকটি প্রযুক্তির সমন্বয় ঘটিয়ে তৈরি করা একটি ব্যবসায়িক মডেল।
৫	সার্ভার (Server)	সার্ভার হল ভোক্তা থেকে অনুরোধ গ্রহন করে সে অনুযায়ী সেবা প্রদানের জন্য সফটওয়্যার। এটা যে কোন কম্পিউটারে চলতে পারে।
৬	ইন্টারনেট যুক্ত সামগ্রী (Internet of Things)	ইন্টারনেট যুক্ত সামগ্রী (Internet of Things, IoT) বলা হয় যেসব ইলেক্ট্রনিক্স সামগ্রীর সাথে ইন্টারনেট সংযোগ থাকে।
৭	উচ্চ-প্রাপ্যতা (High Availability)	উচ্চ প্রাপ্যতা একটি সিস্টেমের বিশেষ বৈশিষ্ট্য, যার লক্ষ সাধারণ সময়ের চেয়ে অধিক সময়ের জন্য প্রযুক্তির প্রাপ্যতা নিশ্চিত করা।
৮	Quality of Service (QoS)	সেবার গুনগতমান (QoS) এমন একটি প্রযুক্তিকে বোঝায়, যা নেটওয়ার্কে প্যাকেট লস, প্যাকেট বিলম্ব কমাতে ডাটা ট্রাফিক পরিচালনা করে। QoS নেটওয়ার্কে নির্দিষ্ট ধরনের প্যাকেটের চলাচলে অগ্রাধিকার প্রদান করে।
৯	দুর্যোগ পুনরুদ্ধার (Disaster Recovery, DR)	দুর্যোগ পুনরুদ্ধার (Disaster Recovery, DR) হল সুরক্ষা পরিকল্পনার একটি অংশ, যার লক্ষ্য হল, উল্লেখযোগ্য নেতিবাচক প্রভাব থেকে প্রযুক্তি সেবাকে দ্রুত পুনরুদ্ধার করে রক্ষা করা।
১০	সেবা স্তরের চুক্তি (SLA)	সেবা স্তরের চুক্তি (SLA) বা Service level Agreement হল প্রযুক্তি সেবা সরবরাহকারী ও এর গ্রাহকদের মধ্যে সম্পাদিত চুক্তি। যেখানে সরবরাহকারী কিভাবে সেবা সরবরাহ করবে, কিভাবে পরিমাপ করবে, কতক্ষণ সরবরাহ করবে, তার বিস্তারিত উল্লেখ থাকে।
১১	PCI DSS	পেমেন্ট কার্ড ইন্ডাস্ট্রি ডেটা সিকিউরিটি স্ট্যান্ডার্ড হল যারা স্বীকৃত ক্রেডিট কার্ড স্কিম পরিচালনা করে, তাদের জন্য একটি তথ্য সুরক্ষা মান।
১২	দুর্যোগ পরবর্তী তথ্য পুনরুদ্ধার (ICT DR)	আইসিটি দুর্যোগ পুনরুদ্ধার হল যে কোন বড় ধরনের ব্যাঘাত বা দুর্ঘটনার পর তথ্য পুনরুদ্ধার প্রক্রিয়া।
১৩	তথ্য প্রতিলিপি (Replication)	সফটওয়্যার বা হার্ডওয়্যার উপাদানের মত নির্ভরযোগ্যতা, ত্রুটি সহনশীলতা বা এক্সেসযোগ্যতার বৃদ্ধি করার জন্য কম্পিউটিং এর প্রতিরূপ।
১৪	অননুমোদিত এক্সেস (Unauthorized	অননুমোদিত এক্সেস হল যখন কেউ কোন ওয়েবসাইট, প্রোগ্রাম, সার্ভার, সেবা বা অন্য কারও অ্যাকাউন্ট বা অন্য কোন পদ্ধতি ব্যবহার করে অন্য

খসড়া

	Access)	সিস্টেমে এক্সেস করতে পারা।
১৫	নিরাপত্তা নিয়ন্ত্রণ কেন্দ্র (Security Operation Center: SOC)	নিরাপত্তা নিয়ন্ত্রণ কেন্দ্র (Security Operation Center: SOC) একটি কেন্দ্রীয় ইউনিট যা প্রযুক্তিগত সুরক্ষার বিষয়গুলো নিয়ে কাজ করে। SOC সেন্টার থেকে এর কর্মীরা প্রযুক্তি ব্যবহার করে সাইটটি তদারকি করে।
১৬	সেবা ব্যত্যয়ের বিস্তৃত আক্রমণ (DDoS)	এটা এমন আক্রমন, যার মাধ্যমে ইচ্ছাকৃতভাবে একাধিক কম্পিউটার সিস্টেম থেকে একযোগে নেটওয়ার্কে ডাটা পাঠিয়ে নেটওয়ার্ককে আকেজো বা ব্যবহার অযোগ্য (Paralyzed) করে রাখা হয়।
১৭	Cloud Service Provider (CSP)	ক্লাউড সেবা সরবরাহকারী, যারা গ্রাহককে সেবা ফি নিয়ে ক্লাউড সেবা দিয়ে থাকে।
১৮	Government of Bangladesh information Security Mannual (GoBISM)	বাংলাদেশ সরকারের তথ্য প্রযুক্তি মন্ত্রনালয়ের আওতাধীন বাংলাদেশ কম্পিউটার কাউন্সিল কর্তৃক প্রণীত বাংলাদেশ সরকার তথ্য সুরক্ষা ম্যানুয়াল GoBISM ভার্সন ১.৫। এটি ২৯ ফেব্রুয়ারী ২০১৬ সালে রিভিউ করা হয়েছে।

খসড়া