গণপ্রজাতন্ত্রী বাংলাদেশ সরকার

ডাটা সেন্টার নির্দেশিকা ২০২০

তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ

ডাক, টেলিযোগাযোগ ও তথ্যপ্রযুক্তি মন্ত্রণালয়

সূচিপত্র:

পটভূমি

বর্তমান সরকার ঘোষিত রূপকল্প-২০২১ তথা ডিজিটাল বাংলাদেশ বিনির্মাণের মাধ্যমে তথ্য-প্রযুক্তি ব্যবহার করে জনগণের দোরগোড়ায় সরকারি সেবা পৌঁছে দেওয়ার অঙ্গীকার ব্যক্ত করা হয়েছে। টেকসই উন্নয়ন অভিষ্ট লক্ষ্যমাত্রা-২০৩০ এর ১৬ (৬)-এ সকল স্তরে কার্যকর, জবাবদিহিতামূলক ও স্বচ্ছ প্রতিষ্ঠানের বিকাশের মাধ্যমে সরকারি সেবার নাগরিক সন্তুষ্টির বিষয়টি বিধৃত হয়েছে। ২০২১ সালে দেশকে একটি সুখী, সমৃদ্ধশালী মধ্যম আয়ের দেশে পরিণত করার লক্ষ্যে সরকারি দপ্তরসমূহ নিরিলসভাবে কাজ করে যাচ্ছে।

বাংলাদেশ সরকার তথ্য ও যোগাযোগ প্রযুক্তি খাতের প্রবৃদ্ধিতে প্রতিশ্রুতিবদ্ধ এবং এ খাতের উন্নয়নে ইতিমধ্যেই সরকার নানা উদ্যোগ গ্রহণ করেছে। এর মধ্যে জাতীয় ডাটা সেন্টার অত্যন্ত কার্যকরী উদ্যোগ। ডিজিটাল প্রযুক্তির অগ্রগতি টেকসই করার লক্ষ্যে তথ্য ও যোগাযোগ প্রযুক্তি বিভাগের আওতাধীন বাংলাদেশ কম্পিউটার কাউন্সিলের তত্ত্বাবধানে জাতীয় ডাটা সেন্টার প্রতিষ্ঠা করেছে।

ডাটা সেন্টার কেন্দ্রিয়ভাবে নিয়ন্ত্রিত কম্পিউটার ও গুরুত্বপূর্ণ টেলিযোগাযোগ ব্যবস্থার সমষ্টি একটা ইনফাস্ট্রাকচার বা কাঠামো, যেখানে সার্ভার, স্টোরেজ ব্যবস্থা, ডাটাবেস, যন্ত্রাংশ, এক্সেস নেটওয়ার্ক, সফটওয়ার এবং আপ্লিকেশন যুক্ত থাকে। এছাড়াও এতে সকল ডাটার ব্যাকআপ, বিদ্যুৎ সরবরাহ, তথ্য আদান প্রদানে প্রয়োজনীয় সংযোগ, পরিবেশ নিয়ন্ত্রণ যেমন শীতাতপ নিয়ন্ত্রণ ও অগ্নি নির্বাপন এবং অনান্য নিরাপত্তা যন্ত্রাংশ থাকে। ডাটা সেন্টার তথ্যপ্রযুক্তিভিত্তিক সেবা যেমন: ক্লাউড সেবা, হোস্টিং সেবা, অধিক সংখ্যক সেবা গ্রহীতার সংযুক্তি, অধিক ভার্চুয়ালইজেশনসহ অনলাইনভিত্তিক কার্যক্রম বাধাহীনভাবে চলতে সহায়তা করে।

তথ্য ও যোগাযোগ প্রযুক্তির সম্প্রসারণ এবং বিপুল পরিমাণ ডাটার উৎপাদন, সংরক্ষণ ও নিরাপত্তাসংক্রান্ত কার্যক্রম সুষ্ঠভাবে সম্পাদনের জন্য তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ হতে এ 'ডাটা সেন্টার নির্দেশিকা ২০১৯' প্রণয়ন করা হয়েছে। এ নির্দেশিকার উদ্দেশ্য হচ্ছে সরকারি প্রতিষ্ঠান বা সংস্থার ডাটা নিরপেক্ষভাবে সংরক্ষণ ও প্রক্রিয়াকরণ, নিরপেক্ষভাবে ডাটা সংরক্ষণের ক্ষেত্রে আন্তর্জাতিক স্বীকৃত মান অনুসরণ, বিভিন্ন জায়গায় বিচ্ছিন্নভাবে ডাটা সংরক্ষণ না করে কেন্দ্রিয়ভাবে সুনির্দিষ্ট মানদন্ড অনুসরণক্রমে ডাটা সংরক্ষণ, ডাটা সংরক্ষণের জন্য যথাযথ মানদন্ড অনুযায়ী যন্ত্রপাতির ব্যবহার নিশ্চিত করা, ডাটা সেন্টারের শ্রেণিবিন্যাস অনুযায়ী আন্তর্জাতিক মানদন্ড অনুসরণপূর্বক ডিজাইন, নকশা ও আনুসাঙ্গিক বিষয়াদির ব্যবহার নিশ্চিত করা এবং দুর্যোগোত্তর তথ্য পুনরুদ্ধারের ক্ষেত্রে যথাযথ প্রক্রিয়া অনুসরণ করা।

দ্রুত পরিবর্তনশীল প্রযুক্তির সঙ্গে তাল মিলিয়ে ডাটা সেন্টার স্থাপন ও পরিচালনায় এ নির্দেশিকাটি সহায়তা করবে।

১. ডাটা সেন্টার (Data Center)

ডাটা সেন্টার হলো ডাটা সংরক্ষণ এবং প্রক্রিয়াকরণের জন্য কেন্দ্রীয়ভাবে স্থাপিত একটি গুরুত্বপূর্ণ স্থাপনা যেখানে সার্ভার, স্টোরেজ ব্যবস্থা, ডাটাবেস, এক্সেস নেটওয়ার্ক, সফটওয়্যার এবং অ্যাপ্লিকেশন সংযুক্ত থাকে। এছাড়াও এতে ব্যাকআপ উপাদান ও বিদ্যুৎ সরবরাহ ব্যবস্থা, তথ্য আদান প্রদানে প্রয়োজনীয় সংযোগ, পরিবেশ নিয়ন্ত্রণ যেমন শীতাতপ নিয়ন্ত্রণ ও অগ্নি নির্বাপন ব্যবস্থা এবং অনান্য নিরাপত্তা যন্ত্রাংশ থাকে।

২. ডাটা সেন্টার নির্দেশিকার উদ্দেশ্য (Purpose of a Data Center Guidlines)

২.১ কোনো প্রতিষ্ঠান বা সংস্থার ডাটা নিরপেক্ষভাবে সংরক্ষণ ও প্রক্রিয়াকরণ নিশ্চিতকরণ;

২.২ ডাটা সংরক্ষণের ক্ষেত্রে আন্তর্জাতিকভাবে স্বীকৃত প্রমিত মান অনুসরণ করা;

২.৩ ডাটা সংরক্ষণের জন্য যথাযথ মানদন্ড অনুযায়ী যন্ত্রপাতির ব্যবহার নিশ্চিত করা;

২.৪ ডাটা সেন্টারের শ্রেণি বিন্যাস অনুযায়ী আন্তর্জাতিক মানদন্ড অনুসরণপূর্বক ডিজাইন, নকশা ও আনুসাঙ্গিক বিষয়াদির ব্যবহার নিশ্চিত করা;

২.৫ দূর্যোগোত্তর তথ্য পুনরুদ্ধারের ক্ষেত্রে যথাযথ প্রক্রিয়া অনুসরণ করা; এবং

২.৬ বিভিন্ন জায়গায় বিচ্ছিন্নভাবে ডাটা সংরক্ষণ না করে কেন্দ্রীয়ভাবে সুনির্দিষ্ট মানদন্ড অনুসরণক্রমে তথ্য সংরক্ষণ করা।

৩. ডাটা সেন্টারের ধরণ (Types of Data Center)

তথ্যের প্রাপ্যতার উপর ভিত্তি করে ডাটা সেন্টারকে ৪ শ্রেণিতে (Tier) ভাগ করা হয়েছে। এক্ষেত্রে শীতলীকরণ, বিদ্যুৎ সরবরাহ, নেটওয়ার্ক যোগাযোগ, সার্বক্ষণিক তদারকিকরণ বিবেচনায় নেয়া হয়। নিচের টেবিলে ডাটা সেন্টারের ধরনগুলিকে Uptime ইনিস্টিটিউট দ্বারা সংজ্ঞায়িত করে;

Tier Requirement	Tier I	Tier II	Tier III	Tier IV
Distribution Path Power and Cooling	1	1	1 active / 1 alternate	2 active
Redundancy active Component	N	N	N+1	2(N+1)
Redundancy backbone	No	No	Yes	Yes
Redundancy horizontal cabling	No	No	No	Optional
Raised Floor	12”	18”	30”-36”	30”-36”
UPS / Generator	Optional	Yes	Yes	Dual
Concurrently Maintainable	No	No	Yes	Yes
Fault Tolerant	No	No	No	Yes
Availability	**99.671%**	**99.749%**	**99.982%**	**99.995%**

N: needed Source: Uptime Institute

৪. মানদন্ড ও প্রত্যয়ন (Standards and Certifications)

৪.১. ডাটা সেন্টারের অবকাঠামোর মানদন্ড (Data Center Infrastructure Standards)

৪.১.১. **Uptime ইনিস্টিটিউটঃ** ডাটা সেন্টারগুলির সঠিক নকশা, নির্মাণ ও কার্যক্রমের জন্য এটি ডাটা সেন্টারের নকশা, নির্মান ও পরিচালনার (Operation) জন্য বিশ্বব্যাপী গৃহীত মানদন্ড:

- **নকশার স্তর প্রত্যয়ন (**Tier Certification of Design Documents**):** ডাটা সেন্টারের স্তর কাঠামো বিন্যাসের প্রথম পদক্ষেপ হল সংস্থার ব্যবহারিক প্রয়োজন অনুযায়ী নকশা প্রস্তুত করা; এবং
- **নির্মিত সেবার স্তর প্রত্যয়ন (**Tier Certification of Constructed Facility**):** প্রক্রিয়ার সর্বশেষ ধাপ হলো নির্মিত ডাটা সেন্টারটি এর প্রত্যয়িত স্তরের মান অনুযায়ী পরিষেবা দিতে পারে তা নিশ্চিত করা।

৪.১.২. **TIA-942**: টেলিযোগাযোগ শিল্প সমিতি (টিআইএ) TIA -942 মানদন্ড নিম্নবর্ণিত বিষয়াদি অন্তর্ভুক্ত করে:

- স্থাপনার আকার এবং বিন্যাস;
- তারের অবকাঠামো (Cabling Infrastructure);
- প্রাপ্যতার নির্ভরযোগ্যতা; এবং
- পরিবেশগত বিবেচনা।

TIA-942-A মানদন্ড তারের অবকাঠামোর সর্বনিম্ন প্রয়োজনীয়তা নির্দিষ্ট করে। নিম্নবর্ণিত স্তর অনুসারে ক্যাবলিং সিস্টেম নির্ধারন করা হয়:

- **প্রথম স্তরঃ (**TIER-I**)** ব্যাকবোন ক্যাবলিং, আনুভূমিক ক্যাবলিং এবং সক্রিয় নেটওয়ার্ক উপাদানগুলি বাড়তি থাকে না। এখানে একটি সহজ তারকা (Star) টোপোলজি ব্যবহৃত হয়। নেটওয়ার্ক কার্যক্রম এতে বাধাগ্রস্ত হতে পারে বিধায়, তথ্য অখন্ডতা নিশ্চিত করা আবশ্যক।
- **দ্বিতীয় স্তরঃ (**TIER- II) ব্যাকবোন এবং অনুভূমিক ক্যাবলিং বাড়তি থাকে না, তবে নেটওয়ার্ক উপাদান এবং তাদের সংযোগগুলি একাধিক হয়। এখানেও একটি তারকা টোপোলজি (Star Topology) ব্যবহৃত হয়; নেটওয়ার্ক কার্যক্রম শুধুমাত্র নির্ধারিত সময়ে বন্ধ করা যেতে পারে;
- **তৃতীয় স্তরঃ** (TIER-III) উভয় ব্যাকবোন ক্যাবলিং এবং সক্রিয় নেটওয়ার্ক উপাদানগুলি এই তারকা টোপোলজিতে বাড়তি (reduntant) থাকে কারণ নেটওয়ার্ক কার্যক্রম অবশ্যই নিরবিচ্ছিন্ন রাখা উচিত; এবং
- **চতুর্থ স্তরঃ** (TIER-IV) ব্যাকবোন ক্যাবলিং এবং সমস্ত সক্রিয় উপাদান যেমন সার্ভার, সুইচ ইত্যাদি অতিরিক্ত থাকতে হবে, 2 x (N + N), সেইসাথে অবিচ্ছিন্ন বিদ্যুৎ সরবরাহ এবং জরুরী বিদ্যুৎ সরবরাহ ব্যবস্থা থাকতে হবে। এই স্তরে (Tier) কোনো SPoF (Single Point of Failur) নেই।

৪.১.৩. **ASHRAE:** আমেরিকান সোসাইটি অফ হিটিং, রেফ্রিজারেটিং অ্যান্ড এয়ার কন্ডিশনার ইঞ্জিনিয়ার্স (ASHRAE) হল তাপ, বায়ু চলাচল, শীতাতপ নিয়ন্ত্রণ এবং হিমায়ন (HVAC&R) পদ্ধতি নকশা ও নির্মাণের তদারকির জন্য একটি বিশ্বব্যাপী পেশাদার সংস্থা। ASHRAE HVAC পদ্ধতির সাথে সম্পর্কিত মান এবং নির্দেশিকা প্রকাশ করে, যা ডাটা সেন্টারে ব্যবহার করার জন্য সুপারিশ করা হচ্ছে।

৪.১.৪. **LEED:** Leadership in Energy and Environmental Design হল বিশ্বব্যাপী ব্যবহৃত সবচেয়ে জনপ্রিয় পরিবেশবান্ধব ভবন প্রত্যয়ন কার্যক্রমগুলির মধ্যে একটি। এটি অলাভজনক মার্কিন গ্রীন বিল্ডিং কাউন্সিল (USGBC) দ্বারা প্রকাশিত, যার লক্ষ্য হল পরিবেশবান্ধব ভবন নকশা, নির্মাণ, পরিচালন ও রক্ষণাবেক্ষণে ভবনের মালিক ও পরিচালকদের পরিবেশগতভাবে দায়বদ্ধ করা এবং দক্ষতার সাথে সম্পদগুলি ব্যবহার করতে তাদের সহয়তা করা। ডাটা সেন্টার স্থাপনা নির্মাণের ক্ষেত্রে এই মানদন্ড অনুসরন করা যেতে পারে।

৪.২. তথ্য নিরাপত্তা সংক্রান্ত মানদন্ডসমুহ (Information Security Related Standards)

৪.২.১. **BDS/IEC 27001:** এই মানদন্ডটি একটি প্রতিষ্ঠানের তথ্য নিরাপত্তা ব্যবস্থাপনা প্রক্রিয়া (ISMS) সম্পর্কিত মৌলিক প্রয়োজনীয়তা বর্ণনা করে। এই মানটি প্রাথমিকভাবে প্রতিষ্ঠানের ব্যবস্থাপনা পরিষদ এবং তথ্য প্রযুক্তি নিরাপত্তা ব্যবস্থাপকদের, এবং দ্বিতীয়তঃ বাস্তবায়ন ব্যবস্থাপকদের, প্রযুক্তিবিদ এবং প্রশাসকদের উদ্দেশ্য করে লেখা। ISMS বাস্তবায়ন অভ্যন্তরীণ ও বহিরাগত নিরীক্ষক দ্বারা নিরীক্ষা করা সম্ভব। ডাটা সেন্টারের তথ্য নিরাপত্তার জন্য এই মানদন্ড অনুসরণ করা যেতে পারে।

৪.২.২. **BDS/IEC 27002:** এটি তথ্য নিরাপত্তা পরিচালনার একটি নির্দেশিকা। মূলত, যেখানে তথ্য সুরক্ষা প্রয়োজন হবে সেখানে এই মান প্রয়োগ করা উচিত। এই মান আইটি নিরাপত্তা ব্যবস্থাপকদের উদ্দেশ্যে তথ্য নিরাপত্তার জন্য প্রণীত।

৪.২.৩. **BDS/IEC 27006:** তথ্য নিরাপত্তা ব্যবস্থাপনা পদ্ধতির নিরীক্ষা মানদন্ড এতে বর্ণীত হয়েছে। (বিসিসি কর্তৃক প্রণয়ণকৃত ISO 27001 Audit Check List 'পরিশিষ্ট-ক' তে অন্তর্ভুক্ত আছে)।

৪.২.৪. **PCI-DSS:** ব্যাংকিং ও আর্থিক প্রতিষ্ঠানসমুহের তথ্য সুরক্ষার জন্য সর্বজনীন মানদন্ড হল PCI-DSS। ব্যাংকিং এবং আর্থিক সিস্টেম ও তথ্য জড়িত থাকলে ডাটা সেন্টারে PCI DSS প্রত্যয়ন গ্রহণ করতে হবে।

৪.২.৫. **BDS/IEC 27033:** তথ্য প্রযুক্তি নেটওয়ার্ক নিরাপত্তাকে লক্ষ্য করে এই মানদন্ডটি প্রণয়ন করা হয়েছে। এতে তথ্য প্রযুক্তি নেটওয়ার্কের কার্যক্রম পরিচালনা ও রক্ষণাবেক্ষণ এবং এর বহির্মুখী সংযোগে নিরাপত্তার বিষয়াবলি আলোচিত হয়েছে।

৪.২.৬. **BDS/IEC 27017:** ক্লাউড কম্পিউটিংএ সংরক্ষিত তথ্যাদির নিরাপত্তা নিশ্চিত করতে এই মানদন্ডটি ব্যবহৃত হয়।

৪.৩. দুর্যোগ পরবর্তী তথ্য পুনোরুদ্ধারের মানদন্ড (Disaster Recovery Standard)

৪.৩.১. **BDS/IEC 24762:** এই মানদন্ড তথ্য এবং যোগাযোগ প্রযুক্তির ক্ষেত্রে দুর্যোগ পরবর্তী তথ্য পুনরুদ্ধার (ICT DR) সেবা বিষয়ক নির্দেশনা প্রদান করে এবং এটি বাস্তবায়নে আবশ্যকীয় ও সর্বোত্তম অনুশীলনসমুহ অন্তর্ভুক্ত করে, উদাহরণস্বরূপ জরুরিভিত্তিতে কম্পিউটার এবং বিকল্প প্রক্রিয়াকরণ স্থাপনাসমুহের প্রাপ্যতা।

৪.৪. নিরবচ্ছিন্ন তথ্য প্রযুক্তি সেবা ব্যবস্থাপনার মানদন্ড (Information Technology Continuity Management Standard)

৪.৪.১. **BDS/IEC 22301:** এটি এমন একটি ব্যবস্থাপনা পদ্ধতির বর্ণনা করে যা তথ্য প্রযুক্তি পরিষেবার নিরবিচ্ছিন্নতা প্রতিষ্ঠা করবে এবং বজায় রাখবে।

৪.৫. ঝুঁকি ব্যবস্থাপনার মানদন্ড (Risk Management Standard)

৪.৫.১. **BDS/IEC 27005:** এই মানদন্ডটি একটি নিয়মতান্ত্রিক, প্রক্রিয়া ভিত্তিক ঝুঁকি ব্যবস্থাপনা বিষয়ে নির্দেশনা দেয় এবং BDS/IEC 27001 মানদন্ড অনুযায়ী ঝুঁকি ব্যবস্থাপনার আবশ্যক চাহিদাগুলিকে সমর্থন করে।

৪.৬. সংস্থার প্রশাসনের জন্য তথ্য প্রযুক্তির মানদন্ড (Organization Governance in Information Technology Standards)

৪.৬.১.**BDS/IEC 38500:** এই মানদন্ডে সংস্থার প্রশাসন সংক্রান্ত তথ্য প্রযুক্তির নিম্নে উল্লিখিত ছয়টি মুলনীতি বর্ণিত হয়েছেঃ

- দায়িত্ব (Responsibility): সংস্থার পরিচালনা পর্ষদ দ্বারা তথ্য প্রযুক্তির যে কোনো বিষয়ে যথেষ্ট গুরুত্ব প্রদান;
- কৌশল (Strategy) : সংস্থার পরিচালন নীতিমালায় তথ্য প্রযুক্তি তথা ডাটা সেন্টার সংক্রান্ত কৌশল অন্তভুক্ত করা। পরিকল্পনা এবং তথ্য প্রযুক্তি কৌশল সংগঠন নীতির নীতিমালায় তথ্য প্রযুক্তির সম্ভাব্যতা এবং কৌশল অন্তর্ভুক্তি;
- অধিগ্রহণ (Acquisition): স্বচ্ছ সিদ্ধান্ত গ্রহণের উপর ভিত্তি করে যথাযথ চাহিদা ভিত্তিক তথ্য প্রযুক্তি বাজেট পরিকল্পনা;
- প্রতিপাদন (Performance): সংস্থার বিভিন্ন বিভাগীয় প্রয়োজনীয়তার সঙ্গে তথ্য প্রযুক্তি সেবাকে পূণর্বিন্যাসকরণ;
- সাদৃশ্য (Conformance): তথ্য প্রযুক্তি ব্যবস্থাকে প্রযোজ্য আইন, বিধান এবং সংস্থার অভ্যন্তরীণ ও বাহ্যিক মানদন্ডের সঙ্গে অনুবর্তি করা; এবং

- মানব আচরণ (Human Behavior): সংস্থার অভ্যন্তরীণ ও বাহ্যিক তথ্য প্রযুক্তি ব্যবহারকারীর চাহিদা বিবেচনা করা।

এই মানদণ্ডটি উপরোক্ত মূলনীতিগুলোর উপর নির্ভর করে তিনটি কাজ আরোপ করেঃ

- মুল্যায়ন (Evaluation): তথ্য প্রযুক্তি কর্মক্ষমতার ধারাবাহিক মুল্যায়ন;
- নিয়ন্ত্রণ (Control): ব্যবসায়িক লক্ষ্যে তথ্য প্রযুক্তির ব্যবহার নিয়ন্ত্রণ; এবং
- পরিবীক্ষন (Monitoring): তথ্য প্রযুক্তির ব্যবহার যথাযথভাবে প্রতিপালন এবং পদ্ধতিগত উৎপাদনশীলতা পর্যবেক্ষণ।

৪.৬.২. **COBIT:** প্রতিষ্ঠানের ব্যবস্থাপনা ও তথ্য প্রযুক্তি বিভাগকে তথ্য প্রযুক্তি প্রশাসন সম্পর্কিত দায়িত্ব সম্পাদনে সাহায্য করার জন্য, ISACA অ্যাসোসিয়েশনের (ইনফরমেশন সিস্টেম অডিট অ্যান্ড কন্ট্রোল এসোসিয়েশন) COBIT তৈরি করেছে, যেখানে তথ্য প্রযুক্তির সকল দিকের একটি সমন্বিত কাঠামো পরিকল্পনা, বাস্তবায়ন এবং হস্তান্তর বিস্তারিতভাবে বিবৃত করা হয়েছে।

৪.৭. তথ্য প্রযুক্তি পরিষেবা ব্যবস্থাপনার মানদণ্ড (Information Technology Service Management Standards)

৪.৭.১ ITIL এবং BDS 20000: এটি তথ্য প্রযুক্তি পরিষেবা পরিচালনার (ITSM) জন্য সেরা পদ্ধতিগুলোর একটি প্রাসঙ্গিক মডেল। ITIL মূলত 'আইটি ইনফ্রাস্ট্রাকচার লাইব্রেরি' থেকে উদ্ভুত, যদিও বর্তমান তৃতীয় সংস্করণটি বৃহত্তর কলেবরে তৈরি। ITIL এর উদ্দেশ্য হল পদ্ধতি, পরিষেবা এবং গ্রাহকদের চাহিদাগুলি অন্তর্ভুক্ত করার জন্য তথ্য প্রযুক্তি প্রতিষ্ঠানগুলোতে প্রযুক্তির বাইরেও সুযোগ সৃষ্টি করা। ITILv3 সংস্করণটি সংগঠন কৌশল সহ তথ্য প্রযুক্তি পরিষেবা পরিচালনার জন্য কৌশলগত পরিকল্পনা প্রক্রিয়ার প্রণয়ন করেছে এবং এভাবে তথ্য প্রযুক্তি সেবা পরিচালনার মান BDS 20000 এর সাথে সামঞ্জস্যতা নিশ্চিত করেছে। এর ৩টি স্তর রয়েছে:

- ভিত্তি স্তর (Foundation);
- মধ্যবর্তী স্তর (Intermediate); এবং
- অগ্রণী স্তর (Advanced)।

ডাটা সেন্টারের আন্তর্জাতিক মানদণ্ড BDS/IEC 20000 অনুযায়ী এর কার্যক্রম পরিচালনার প্রত্যয়ন থাকতে পারে।

৪.৮. মান নিয়ন্ত্রণ ব্যবস্থাপনার মানদণ্ড (Quality Management Standard)

৪.৮.১. **BDS 9001:** ডাটা সেন্টারের মান নিয়ন্ত্রণের জন্য প্রয়োজনীয় শর্তাদি এই মানদণ্ড বর্ণনা করে।

৪.৯. পরিবেশগত ব্যবস্থাপনার মানদণ্ড (Environmental Management Standard)

৪.৯.১. **BDS 14001:** পরিবেশগত মান নিয়ন্ত্রণের জন্য প্রয়োজনীয় শর্তাদি এই মানদণ্ড বর্ণনা করে।

৫. পরিকল্পনা ও নকশা (Planning and Designing)

ক্লাউড কম্পিউটিং, ইন্টারনেটযুক্ত সামগ্রী (IoT) এবং বৃহত্তাকার তথ্যভান্ডার দ্বারা সৃষ্ট নতুন সংযোগ এবং প্রক্রিয়াকরণের চাহিদা পূরণের জন্য গতি, দক্ষতা, নমনীয়তা এবং কর্মক্ষমতা সম্প্রসারণ ইত্যাদি বিবেচনা করে পরিকল্পনা ও নকশা প্রনয়ণ করা প্রয়োজন।

৫.১. পরিকল্পনার ক্ষেত্রে বিবেচ্য বিষয়সমূহ (Planning Concerns)

একটি ডাটা সেন্টার স্থাপনা সংস্কার, সম্প্রসারণ বা স্থানান্তরের সুযোগ সুবিধা, কার্যক্ষমতা ও সক্ষমতার বিষয় বিবেচনা করে পরিকল্পনা গ্রহণ আবশ্যক ।

একটি সফল ডাটা সেন্টার স্থাপনার মূলমন্ত্র হলো, যা দীর্ঘমেয়াদে টেকসই, সরঞ্জাম এবং কার্যক্রমের জন্য একটি ধারক হিসাবে বিবেচিত, সেইসঙ্গে একটি সমন্বিত প্রক্রিয়া, যার প্রতিটি উপাদানের নমনীয়তা এবং কর্মক্ষমতা সম্প্রসারণযোগ্যতা বিবেচনা করা প্রয়োজন।

ডাটা সেন্টার পরিকল্পনার ক্ষেত্রে বিবেচ্য বিষয়সমূহ:

- নতুন সরঞ্জাম (New equipment);
- দৃঢ়করণ এবং সম্প্রসারণ (Consolidations and expansions);
- নতুন বিকল্প সৃষ্টির প্রয়োজনীয়তা (New redundancy requirements);
- ক্রমবর্ধমান বিদ্যুৎ চাহিদা (Incremental power requirements);
- নিরাপত্তার নতুন শর্তাদি (New security requirements);
- ক্রমবর্ধমান শীতলীকরণের চাহিদা (Incremental cooling demands);
- অপ্রতুল মেঝের আকার (Constrained floor space);
- নিরাপত্তা ব্যবস্থা এবং সুরক্ষার নতুন প্রবিধান (New safety and security regulations);
- পরিচালনা পদ্ধতির পরিবর্তন (Changes in operational procedures);
- লক্ষ্যের পরিবর্তন (Changes in mission); এবং
- খরচের চাপ (Cost pressures)।

কর্ম পরিকল্পনাঃ অবস্থান, ভবন নির্বাচন, স্থান বিন্যাস এবং ভবনের নকশা সহ ডাটা সেন্টার স্থাপনার সকল দিকগুলি নমনীয় ও সম্প্রসারণযোগ্য হতে হবে।

৫.২. নকশার বিবেচ্য বিষয় (Design Concerns)

যেহেতু ডাটা সেন্টার সর্বদা পরিবর্তন এবং পরিবর্ধনশীল, তাই অত্যাধিক মূলধন ব্যয় এড়াতে একটি নমনীয় নকশা পদ্ধতির প্রয়োজন হয়। ভাল নকশা সাধারণত ক্ষতি রোধ করতে সহয়তা করে এবং অভিযোজনযোগ্য (Adaptable), মডুলার নকশার সাহায্যে বর্তমান ও ভবিষ্যতের লক্ষ্য বাজেটের মধ্যেই পুরণ করা সম্ভব।

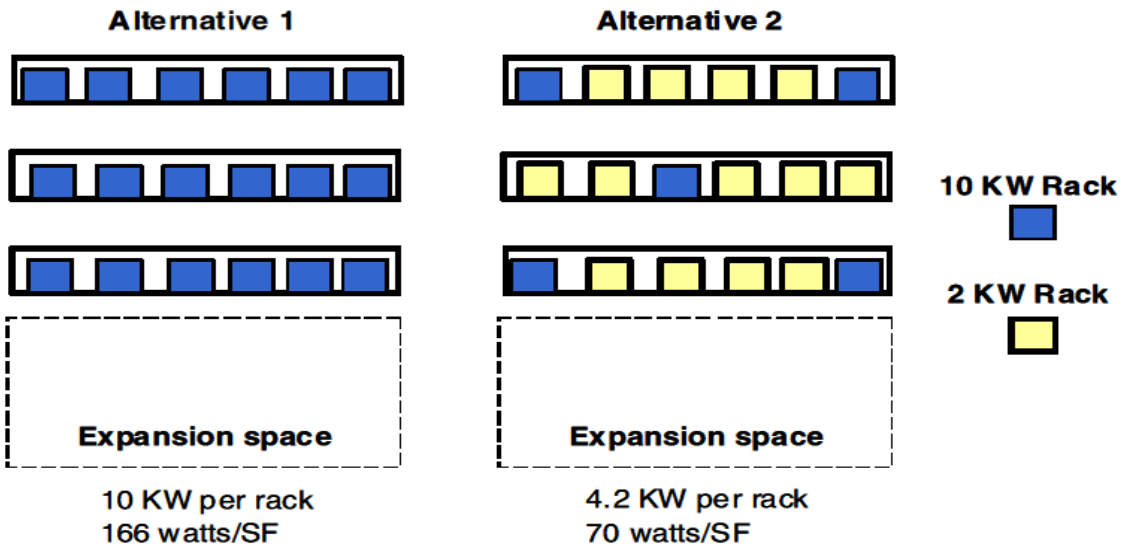
৫.২.১. ঘনত্ব বনাম ধারণক্ষমতা (Density vs. Capacity)

এই বিষয়ে বহু প্রমাণ পাওয়া যাচ্ছে যে, ডাটা সেন্টারগুলি উচ্চ বিদ্যুৎ ক্ষমতার জন্য নকশা করা হচ্ছে, কারণ বর্তমানের কম্পিউটিং ও সংরক্ষক যন্ত্রাংশগুলির শক্তি সরবরাহ এবং শীতলীকরণের চাহিদা বৃদ্ধি পাওয়া। সরঞ্জামের প্রাথমিক ও দীর্ঘমেয়াদি বৈদ্যুতিক ক্ষমতার উপর নজর দেয়া উচিত। কম্পিউটার সরঞ্জামের জন্য বর্গ ফুট প্রতি ৭০ ওয়াট বৈদ্যুতিক ক্ষমতা সাধারণত প্রয়োজন হয়। তবে, শীতাতপ নিয়ন্ত্রণ, আর্দ্রতা, আলো, ও অবিচ্ছিন্ন শক্তি সরবরাহ (ইউপিএস) এর জন্য প্রয়োজনীয় অতিরিক্ত বিদ্যুৎ চাহিদা ট্রান্সফরমারের ক্ষতির কারণ হতে পারে। এই অতিরিক্ত চাহিদা সরঞ্জাম বসানো এবং বায়ু-পরিচালনা দক্ষতার উপর নির্ভর করে বিদ্যুৎ ব্যবহারে দেড় গুণ বেশি ওয়াটেজ যুক্ত করতে পারে।

কর্ম পরিকল্পনাঃ ডাটা সেন্টারে ঘনত্ব বনাম ধারণক্ষমতার দিকে নজর দেওয়া এবং উষ্ণ ও শীতল র‍্যাকের সারির (Rack aisle) মধ্যে যথেষ্ঠ দূরত্ব রাখা, এতে বায়ুপ্রবাহ বৃদ্ধির মাধ্যমে তাপ উৎপাদন হ্রাস পাবে।

৫.২.২. র‍্যাকের বিন্যাস (Rack Layout)

আধুনিক সার্ভার এবং সংরক্ষক যন্ত্রাংশগুলি একই র‍্যাকের মধ্যে রাখা যেতে পারে যার ফলে প্রতি র‍্যাকে বিদ্যুৎ চাহিদা ১৮ থেকে ২০ কিলোওয়াট হবে। উচ্চ ক্ষমতা সম্পন্ন সার্ভার এবং সংরক্ষক যন্ত্রাংশগুলি ঘনভাবে স্থাপনের প্রাথমিক সমস্যাটি হলো, এটি জায়গার ব্যাপারে কার্যকর হলেও, উচ্চ তাপমাত্রার কারণে অতিরিক্ত শীতলীকরণের প্রয়োজন হয় যা উল্লেখযোগ্যভাবে বৈদ্যুতিক খরচ বৃদ্ধি করে।



উপরের চিত্রে একটি র‍্যাকের বিন্যাসের আলোকে বিদ্যুৎ চাহিদাকে দেখানো হয়েছে। একটি ঘন-স্থাপন পদ্ধতির বিকল্প বিন্যাস হলো উচ্চ এবং নিম্ন ঘনত্বের মিশ্রণ। উপরের চিত্রের প্রথম সজ্জায়, র‍্যাকে উচ্চ-ঘনত্বের সার্ভারগুলিকে একত্রে রাখা হয়েছে, যেখানে প্রতি বর্গ ফুটে ১৬৬ ওয়াট বৈদ্যুতিক ক্ষমতা প্রয়োজন। দ্বিতীয় সজ্জায়, উচ্চ-এবং নিম্ন-ঘনত্বের র‍্যাকের মিশ্রণটিতে বর্গ ফুট প্রতি ৭০ ওয়াট বৈদ্যুতিক ক্ষমতার প্রয়োজন। র‍্যাকের পরিবর্ধিত অংশে প্রতি বর্গ ফুটে অতিরিক্ত ৩০ ওয়াট পর্যন্ত (বর্গ ফুট প্রতি ১০০ ওয়াটের অনুকূলতা অনুমান করে) বৈদ্যুতিক ক্ষমতা বৃদ্ধিতে সহয়তা করে। প্রথম সজ্জায়, বৈদ্যুতিক চাহিদা ইতিমধ্যে এই সীমারেখা অতিক্রম করে, যাতে অতিরিক্ত বৈদ্যুতিক এবং শীতলীকরণ ক্ষমতা যোগ ছাড়া পরিবর্ধন করা অসম্ভব।

কর্ম পরিকল্পনাঃ উচ্চশক্তির সার্ভারকে ঘনভাবে র‍্যাকে রাখা থেকে বিরত থাকতে হবে; উচ্চ ও নিম্ন ঘনত্বের র‍্যাকগুলোকে মিশিয়ে রাখা উচিত যাতে উচ্চ ক্ষমতার সার্ভারগুলি দ্বারা উৎপাদিত তাপের প্রভাব কমে আসে। সম্ভব হলে ঘন সজ্জার পরিবর্তে ছড়িয়ে রাখা ভালো ।

৫.২.৩. র‍্যাকের সারি (Rack Units)

সাধারণত, স্থাপনা পরিকল্পনাকারীরা ডাটা সেন্টারের ক্ষমতা পরিমাপ করার জন্য প্রতি র‍্যাকের ক্ষেত্রফল (বর্গফুট) বা ওয়াট (Watt) প্রতি বর্গফুট হিসাবে স্থান পরিকল্পনা করেন। এই পদ্ধতির সমস্যা হলো, এটি উচ্চ-ঘনত্বের র‍্যাকের বিন্যাস থেকে নির্গত শক্তির তীব্রতা হিসাব করতে ব্যর্থ হয়। বর্গফুট প্রতি ওয়াটের এক র‍্যাকের বিন্যাস (Rack Configuration) থেকে অন্যটির পার্থক্য সনাক্ত করতে ব্যর্থ হয়, যেখানে উল্লেখযোগ্য উত্তপ্ত এলাকা (Hot Spot) ক্রমান্বয়ে শীতাতপ নিয়ন্ত্রণের (Air Condition) প্রয়োজন হতে পারে। তাই র‍্যাকের বিন্যাসের ভিত্তিতে একটি ডাটা সেন্টার পরিকল্পনা করার পরামর্শ দেওয়া হয়। এই কৌশলে প্রতিটি র‍্যাকের বিন্যাস শীতাতপ নিয়ন্ত্রণের জন্য সরঞ্জাম এবং ক্রমবর্ধমান বিদ্যুতের (অর্থাৎ ৬০ শতাংশ) ব্যবহার আনুযায়ী মোট-ওয়াটেজের দৃষ্টিকোণ থেকে হিসাব করা হয়।

Example

Power per Rack	Watts
Server blade enclosure	50
Patch panel power	25
Wattage per server	43
x 10 servers per enclosure	430
Total wattage per enclosure	505
x five enclosures per rack	2,525
Add energy factor for HVAC power (60 percent)	1,515
Total Wattage per Rack	**4,040**

Goal:
Maintain an *average* of 4 kilowatts per rack over the raised floor

Total Space and Power Over Raised Floor (Base Case) — 200 Racks

Space	6,000 square feet (200 x 30 square feet)
Expansion space	6,000 square feet (double the rack footprint for growth capacity during a 10-year period)
Total space	12,000 square feet
Power	808,000 watts
Watts per SF	67 watts (Use a design envelope of between 50 watts and 100 watts per square foot.)

উপরের উদাহরণটিতে দেখা যায় যে মোট র‍্যাকের (Rack) সংখ্যা গণনা করে, মোট কিলোওয়াট এবং ব্যবহৃত স্থান হিসাব করা যায়। উপরের উদাহরণে, ২০০ র‍্যাক বিন্যাস, প্রতি বিন্যাসে ১০টি সার্ভার, ফলে মোট ১২০০০ বর্গফুট স্থান প্রয়োজন হয় এবং ৮০৮ কিলোওয়াট বা ৬৭ ওয়াট প্রতি বর্গফুট মোট শক্তি (Power) প্রয়োজন হয় যা বর্গ ফুট প্রতি পরিকল্পিত ৫০ থেকে ১০০ ওয়াটের মধ্যে আছে। যদি গড় বিদ্যুৎ চাহিদা র‍্যাক প্রতি ৪ কিলোওয়াট অতিক্রম করে তবে বুঝা যায় যে র‍্যাকের সারিটি পুনঃবিন্যাস করা উচিত, অথবা সামগ্রিক ব্যয় সক্ষমতা বৃদ্ধি করার জন্য বিন্যাসে (Layout) অতিরিক্ত স্থান যুক্ত করা উচিত।

কর্ম পরিকল্পনাঃ ডাটা সেন্টারের মোট স্থান এবং বিদ্যুৎ চাহিদা হিসাব করার জন্য র‍্যাকের বিন্যাসকে পরিকল্পনার মৌলিক উপাদান হিসাবে ব্যবহার করা।

৫.২.৪. প্রাপ্যতা এবং ত্রুটি সহনশীলতা (Availability and Fault Tolerance)

Uptime ইনিস্টিটিউট চারটি ত্রুটি সহনশীলতা এবং প্রাপ্যতার উপর ভিত্তি করে ডাটা সেন্টারের চারটি স্তর (Tier) এ ভাগ করেছে। প্রথম স্তর (Tier I) হল সর্বনিম্ন স্তর, এবং চতুর্থ স্তর (Tier IV) হল সর্বোচ্চ, যাতে একাধিক পথে বিদ্যুৎ বিতরণ, উৎপাদন এবং ইউপিএস যন্ত্রাদি সংযুক্ত থাকে। প্রথম স্তর (Tier I) ২৮.৮ ঘন্টা পর্যন্ত বার্ষিক ব্যর্থতা (Outage) নির্দেশ করে; দ্বিতীয় স্তর (Tier II) ২২ ঘন্টা নির্দেশ করে; তৃতীয় স্তর (Tier III) ১.৬ ঘন্টা এবং চতুর্থ স্তর (Tier IV) শুধুমাত্র ০.৪-ঘন্টা বার্ষিক ব্যর্থতা বা ৯৯.৯৯৫% প্রাপ্যতা নির্দেশ করে। একটি ডাটা সেন্টারের স্তর (Tier), এর নকশার বিবরণীকে (Specification) প্রভাবিত করে। স্তরের (Tier) মান যত বেশী, নির্মাণ ও পরিবেশগত সরঞ্জাম তৈরির জন্য বিনিয়োগও তত বেশী। স্তরের ত্রুটি সহনশীলতা ডাটা সেন্টার পরিচালনার জটিলতা নির্ধারণ করে। Uptime ইনিস্টিটিউট সতর্ক করেছে যে, নকশার বিবরণী দিয়ে প্রাপ্যতার স্তরীকরণ নিশ্চিত করা যায় না। অধিকাংশ পরিষেবার ব্যাঘাত ঘটে মানুষের সৃষ্ট ত্রুটির কারণে। সুতরাং, নিয়োগ, দক্ষতার বিকাশ, প্রশিক্ষণ এবং একটি ইতিবাচক কর্ম পরিবেশের দিকে মনোযোগের মাধ্যমে ত্রুটিহীনতা, উচ্চ-প্রাপ্যতা (High Availability) নিশ্চিত করা সম্ভব।

কর্ম পরিকল্পনাঃ নকশার বিবরণী অনুযায়ী ত্রুটি সহনশীলতা নির্ণয় করতে হবে।

৬. বাহ্যিক অবকাঠামো (Physical Infrastructure)

৬.১. অবস্থান (Site)

একটি ডাটা সেন্টারের অবস্থান ব্যাপকভাবে এর নিরাপত্তা, কর্মদক্ষতা এবং পরিচালনার ব্যয়কে প্রভাবিত করে। স্থাপনা নির্বাচনের মানদন্ডের একটি তালিকা নিম্নে সুপারিশ করা হলো:

- আবাসিক বা অন্যান্য শব্দ সংবেদনশীল এলাকার কাছাকাছি না হওয়া;
- পার্কিং, পানি সঞ্চয়স্থান, জ্বালানী সঞ্চয়স্থান, ট্রান্সফরমার বা সাবস্টেশন বা জেনারেটর বসানোর জায়গা থাকতে হবে;
- সরঞ্জাম সরবরাহের জন্য ট্রাক প্রবেশের ব্যবস্থা থাকতে হবে;
- ডাটা সেন্টারের স্থাপনা থেকে সরঞ্জামাদি সহজে পরিবহনের সুযোগ সুবিধা;
- কম্পন এবং ঝুঁকি উৎস (যেমন বিমানবন্দর এবং রেল লাইন) থেকে দূরে অবস্থিত হতে হবে;
- হাসপাতাল, পুলিশ ফাঁড়ি, রাজনৈতিক স্থাপনা ইত্যাদি সংকটপূর্ণ এলাকা পরিহার করতে হবে;
- একাধিক বিদ্যুৎ সরবরাহ গ্রিড বা বিদ্যুৎ উৎপাদন কেন্দ্রের থেকে সহজে বিদ্যুৎ সংযোগ পাওয়া যায় এমন এলাকা হবে;
- বন্যাপ্রবণ সমভূমি এবং টর্নেডো এবং হারিকেন-প্রবণ এলাকার বাইরে অবস্থিত হতে হবে; এবং
- স্থানীয় কর্তৃপক্ষ বিল্ডিং ব্যবহার করার এখতিয়ার রাখে।

৬.২. স্থাপত্য (Architecture)

ভবনের ধরণ উল্লেখযোগ্যভাবে দখলিস্বত্তের খরচ, নিরাপত্তা, সম্প্রসারন এবং কর্মক্ষমতার নমনীয়তা প্রভাবিত করতে পারে। স্থাপত্যের নিম্নবর্ণিত মানদন্ড সুপারিশ করা হল:

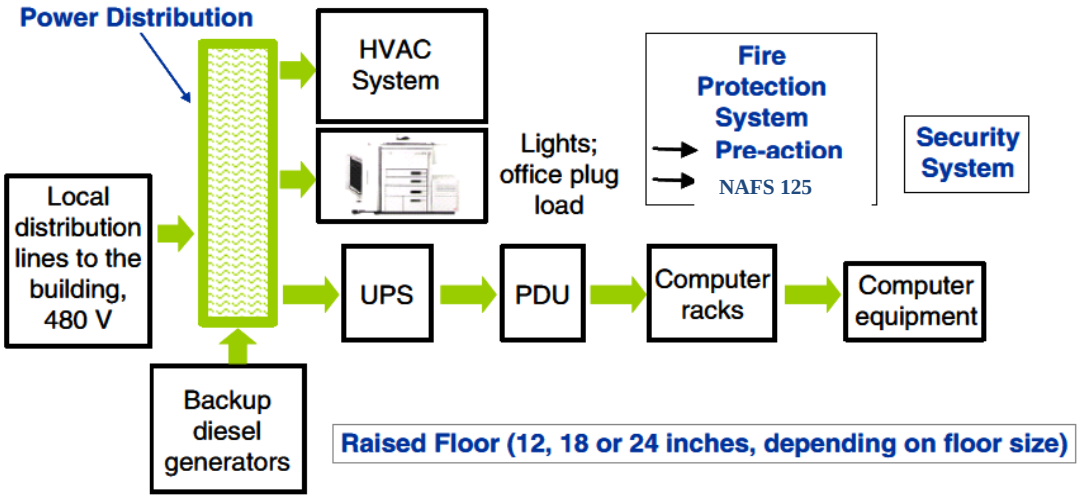
- বৃহৎ কলামের দূরত্ব (৩০ ফুট X ৫০ ফুট উত্তম);
- কাঠামোগত মেঝে (Slab) থেকে সর্বনিম্ন কাঠামোগত অংশের উচ্চতা ন্যূনতম ১৩ ফুট;
- কার্যকরী মেঝে ফলক (আয়তাকার, বর্গাকার বা পার্শ্ব কোর অগ্রাধিকারযোগ্য);
- ন্যূনতম কপাট সুবিধা; শক্তপোক্ত ও অগ্নিরোধী হতে হবে;
- ভাল ছাদ – আকাশপ্রদীপ (Skylight) ছাড়া ছাদ;
- সরঞ্জাম পরিবহনের জন্য পন্য উঠানামা করার স্থান এবং ইউপিএসের ব্যাটারী ও অন্যান্য ভারি দ্রব্যাদি পরিবহণের জন্য ট্রলির ব্যবস্থা;
- ফর্কলিফটের দ্বারা পণ্য ডাটা সেন্টারের অভ্যন্তরে পণ্য পরিবহণের জন্য প্রয়োজনীয় ঢালু সিড়ির ব্যবস্থা;
- কঠিন আবর্জনা অপসারণের ব্যবস্থা;
- একক স্থান দিয়ে প্রবেশ এবং ভবনের আশেপাশে যথেষ্ট নিরাপত্তার ব্যবস্থা;
- জরুরি নির্গমণ ব্যবস্থা;
- শুধুমাত্র একাধিক তলার জন্য: প্রাথমিক / জরুরী বিদ্যুৎ বিতরণ, বিভিন্ন তারের ঢোকার এবং অন্যান্য উল্লম্ব পরিষেবাগুলির জন্য ভবনে পর্যাপ্ত এবং একাধিক উত্থানোপযোগীতা (Riser) নিশ্চিত করা আবশ্যক (অধিক তথ্যের জন্য পরিশিষ্ট দ্রষ্টব্য);
- ছাদে বজ্রপাত নিঃসরণের জন্য বজ্র নিরোধক দন্ডের (Lightening Rod) ব্যবস্থা;
- ছাদের উপর যান্ত্রিক সরঞ্জাম স্থাপনের জন্য শাব্দিক এবং নান্দনিক ঢাকনার (Screening) ব্যবস্থা; এবং
- ৫০০০ থেকে ২০০০০ বর্গ ফুট ব্যবহারযোগ্য স্থান হলে ভাল হয়।

৬.৩. ভবনের গুরুত্বপূর্ণ ব্যবস্থাসমুহ (Critical Building System)

বৈদ্যুতিক শক্তি, স্থান বরাদ্দকরণ এবং যান্ত্রিক প্রক্রিয়াগুলির সর্বোত্তম ব্যবহারের নিমিত্তে একটি সমন্বিত পদ্ধতি হিসাবে ডাটা সেন্টারটি নকশা এবং বাস্তবায়ন করতে হবে। পাঁচটি গুরুত্বপূর্ণ ভবন নির্মাণ প্রক্রিয়া একটি ডাটা সেন্টারে সুবিস্তৃত প্রকৌশল থাকা প্রয়োজন:

- বিদ্যুৎ উৎস (Power source) – বিদ্যুতের জন্য সাবস্টেশন, ইউ.পি.এস, বিকল্প ডিজেলের জেনারেটর, বিদ্যুৎ বিতরণ ব্যবস্থা (PDU) এবং মধ্যবর্তী বিতরণ ব্যবস্থাসহ বিদ্যুৎ বিতরণ;
- তাপ, বায়ু চলাচল এবং এয়ার কন্ডিশনার (HVAC) পদ্ধতি - এটি ছাদে স্থাপিত সুবিস্তৃত ব্যবস্থা যা স্থানীয়ভাবে বায়ু শীতলীকরণ করে। উত্থিত মেঝের নিচ দিয়ে বায়ু সঞ্চালন সমানভাবে বায়ু বিতরণের একটি কার্যকর উপায় হতে পারে। সমসাময়িক ডাটা সেন্টারে সম্ভবত প্রধান সমস্যা আধুনিক সার্ভার এবং তথ্য সংরক্ষক যন্ত্রাংশের তীব্র তাপ উৎপাদনের বিপরীতে পর্যাপ্ত শীতলতা এবং বায়ু চলাচল বজায় রাখা;
- অগ্নি সুরক্ষা ব্যবস্থা (Fire protection systems) - সংবেদনশীল এলাকা যেমন ডিস্ক স্টোরেজ এলাকার জন্য শুষ্ক ও সিক্ত অগ্নি নির্বাপক পদ্ধতিগুলির আন্তঃসংযোগ থাকা উচিত;
- নিরাপত্তা ব্যবস্থা (Security systems) - স্থানীয় এবং কেন্দ্রীয় প্রহরার ব্যবস্থা এবং অ্যাক্সেস কন্ট্রোল সিস্টেম দ্বারা এর ব্যবহার সীমিত হবে; এবং
- উত্থিত মেঝের ব্যবস্থা (Raised floor systems) এবং বায়ু সঞ্চালনের জন্য ছিদ্রযুক্ত উত্থিত মেঝের (Perforated Raised Floor) ব্যবস্থা।

নিচের ছবিতে ভবনের গুরুত্বপূর্ণ ব্যবস্থাসমুহ দেখানো হলঃ



৬.৪. বিদ্যুৎ বিতরণ (Power Distribution)

ডাটা সেন্টারের নির্ভরযোগ্যতা এবং কর্মদক্ষতার জন্য বিদ্যুৎ উৎপাদন এবং বন্টন ব্যবস্থা অত্যন্ত গুরুত্বপূর্ণ। প্যাচ ফলক (patch panels) এবং বৈদ্যুতিক তারের আবরক নলের (conduits) মতো প্রধান বৈদ্যুতিক উপাদানগুলোতে অধিক সক্ষমতা দেয়া এবং বৈদ্যুতিক চাহিদার ভবিষ্যৎ বৃদ্ধির সাথে তাল মেলানোর জন্য উচ্চমানের বৈদ্যুতিক তারের ব্যবহার করা অপরিহার্য। ডাটা সেন্টারের বিদ্যুৎ বিতরণ ব্যবস্থা নির্মাণের জন্য নিম্নবর্ণিত অনুশীলনসমুহ সুপারিশ করা হল:

- সামগ্রিক বিদ্যুৎ চাহিদার মূল্যয়ন (অর্থ্যাৎ, র‍্যাক প্রতি ব্যবহারের পরিমাপ);

- পরিষেবাগুলিতে একাধিক বৈদ্যুতিক সংযোগ নিশ্চিত করা;
- রক্ষণাবেক্ষণের জন্য বাইপাস এবং জরুরি সংযোগ বিচ্ছিন্নকরণ (Shutdown) সুবিধা;
- সরঞ্জামগুলোর একক বা তিন ফেজে বিদ্যুতের প্রয়োজন নিরুপন করা;
- গ্রাউন্ডিং এবং বন্ডিংয়ের (grounding and bonding) জন্য প্রাসঙ্গিক বাংলাদেশী বা আন্তর্জাতিক মানদণ্ড মেনে চলা এবং মেস (Mesh) সংযোগ আকারে গ্রাউন্ডিং করা;
- ভবিষ্যতে সম্প্রসারণ জন্য উচ্চমানের তারের ব্যবহার;
- উচ্চ কম্পাংকের প্রতিবন্ধকতা (high-frequency impedance) কমানোর জন্য একটি প্রাসঙ্গিক সাংকেতিক গরাদ (SRG) সরবরাহ করা উচিত;
- বর্তনী বিচ্ছিন্নকারক (circuit breakers) এবং সরঞ্জাম সংযোগ সংহত করার জন্য বিদ্যুৎ বিতরণ যন্ত্র (PDUs) ব্যবহার করা;
- স্থির বৈদ্যুতিক নিঃসরণ (electrostatic discharge) কমানোর জন্য আপেক্ষিক আর্দ্রতা মাত্রা বজায় রাখা;
- তড়িৎ চৌম্বকীয় হস্তক্ষেপ (EMI) কমানোর জন্য সচেতন হতে হবে; প্রয়োজনে এ থেকে রক্ষা পাওয়ার উপায় বের করা;
- বিদ্যুৎ সর্তকরণ (power-conditioning) সরঞ্জাম ব্যবহার করা বা অবিচ্ছিন্ন বিদ্যুৎ সরবরাহ যেমন, UPS ব্যবস্থায় তা একীভুত করা; এবং
- ভোল্টেজের হঠাৎ বৃদ্ধি প্রতিরোধ (TVSS) ব্যবস্থা ব্যবহার করা।
- ট্যাপ অফ বাক্সের সাহায্যে বাস বার ট্রাংকের মাধ্যমে প্রধান বিতরণ বোর্ডের (MDB) সঙ্গে র‍্যাকের বিদ্যুৎ বিতরণ ইউনিট (PDU) যুক্ত করা।

৬.৫. বিদ্যুৎ সরবরাহ (Power Supply)

ইউপিএস - এবং, অনেক ক্ষেত্রে, বিকল্প ডিজেল চালিত জেনারেটর - সর্বজনীন ব্যবহৃত বিদ্যুতের ব্যতয় ঘটলে বিদ্যুতের নিরবিচ্ছিন্ন প্রবাহ বজায় রাখার জন্য অত্যন্ত গুরুত্বপূর্ণ। ডাটা সেন্টারের বিদ্যুৎ সরবরাহ সম্পর্কিত নিম্নবর্ণিত অনুশীলনগুলি সুপারিশ করা হলো:

- **নিরবিচ্ছিন্ন বিদ্যুৎ সরবরাহ (UPS):**
    - কমপক্ষে ২ ঘন্টা পর্যন্ত ১০০% বিদ্যুৎ চাহিদা পুরণের ক্ষমতা;
    - ডাটা সেন্টারের স্তর (Tier) অনুযায়ী লোড ব্যালান্সিং এর জন্য বিকল্প UPS এর ব্যবস্থা;
    - এছাড়াও সর্বোচ্চ (Peak) লোড বা ত্রুটিপূর্ণ ওভারলোড অবস্থার জন্য প্রয়োজনীয় আকার; এবং
    - সর্বদা বিদ্যুৎ ফিল্টারের নিয়ন্ত্রণ কার্যকর রাখা।
- **বিকল্প বিদ্যুৎ উৎপাদক (Backup Generator)**:
    - তৃতীয় স্তর (Tier III) এবং চতুর্থ স্তর (Tier IV) মানের ত্রুটি সহনশীলতা অর্জন করার জন্য প্রয়োজন;
    - ২ ঘন্টার বেশি সময় বিদ্যুৎ অনুপস্থিতিতে কাজ করতে সক্ষম;
    - জ্বালানি সংরক্ষণ এবং শব্দদূষণ হ্রাসে সংশ্লিষ্ট নীতিমালা বিবেচনা করা;
    - নিষ্কাশন এবং কম্পনের প্রভাব বিবেচনা করা;
    - ডিজেল জ্বালানি ক্রয়ের জন্য জ্বালানি পরিবেশকের সাথে চুক্তি করা এবং তা সংরক্ষণ ও রক্ষণাবেক্ষণের জন্য জ্বালানি ট্যাংকের ব্যবস্থা করা; এবং
    - জেনারেটরের নিয়মিত পরীক্ষার জন্য পরিকল্পনা করা।

ডাটা সেন্টারের জন্য ভবনের বিদ্যুৎ সরবরাহ উৎস একটি নিবেদিত LT প্যানেলে যুক্ত করা উচিত। LT প্যানেলটি অবশ্যই প্রয়োজনীয় সংযোগ এবং TPN Bus Bar এর সাথে প্রয়োজনীয় অন্তর্গামী MMSB অন্তর্ভুক্ত থাকা উচিত। ইউ.পি.এস,

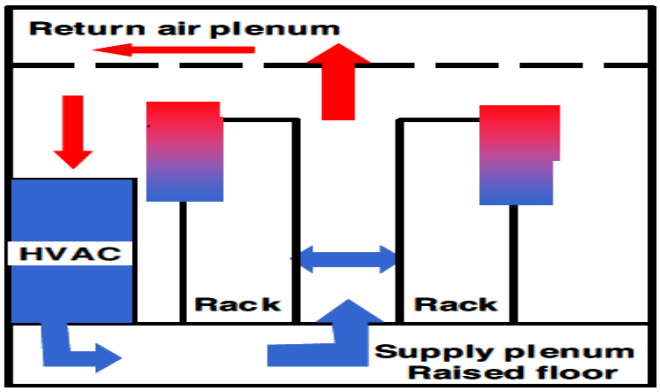
শীতাতপ নিয়ন্ত্রণ, আলো এবং কাঁচামালের মতো বিভিন্ন লোডগুলির জন্য ভিন্ন নিয়ন্ত্রণ ব্যবস্থা থাকা উচিত। উপরের কাঠামোর ভিত্তিতে, তার এবং এর আকার প্রয়োজন অনুযায়ী ব্যবহার করতে হবে।

৬.৬. শীতলীকরণ ব্যবস্থা (Cooling System)

আধুনিক উচ্চ-ঘনত্ব সার্ভার এবং তথ্য সংরক্ষক (Storage) প্রযুক্তিগুলির ক্রমবর্ধমান তাপ উৎপাদন ডাটা সেন্টার শীতলীকরণের জন্য একটি গুরুত্বপূর্ণ সমস্যা হয়ে দাড়িয়েছে। একটি HVAC পদ্ধতি নকশা করতে নিম্নের নির্দেশিকা অনুসরণ করা যেতে পারে:

- একটি সহনশীল তাপমাত্রা নিশ্চিত করা - ১৮ থেকে ২২ ডিগ্রি সেলসিয়াস;
- আপেক্ষিক আর্দ্রতা - ৪৫ শতাংশ থেকে ৫০ শতাংশ;
- নীচে থেকে উপর পর্যন্ত বায়ু প্রবাহ;
- কেন্দ্রীভূত পদ্ধতি এড়িয়ে চলা – বিস্তৃত ব্যবস্থা (Distributed Unit) নির্বাচন করা;
- শীতল পার্শ্ব / উত্তপ্ত পার্শ্ব র‍্যাক (Rack) বিন্যাস ব্যবহার করা;
- কক্ষচাপের উপরে ৫ শতাংশ স্থিতিচাপ বজায় রাখা;
- উত্থিত মেঝেতে (Raised floor) বায়ু নির্গমনের ছিদ্র এড়ানো;
- উষ্ণ ও শীতল বায়ুর মিশ্রণ পরিহারপুর্বক বায়ু সঞ্চালণের ব্যবস্থা করা;
- প্রয়োজনমত শীতলীকরণ স্থান ব্যবহার; এবং
- দরজা, অস্থায়ী মেঝে এবং এর আশেপাশের এলাকায় বাষ্প বাধা বজায় রাখা।

নিচের চিত্রে একটি শীতলীকরণ ব্যবস্থা দেখানো হলঃ



৬.৭. উত্থিত মেঝে (Raised Access Floor (RAF))

উত্থিত মেঝে বৈদ্যুতিক এবং সংকেতবাহী তারের ব্যবস্থাপনার জন্য সবচেয়ে কার্যকর এবং ব্যয়সাধ্য সমাধান প্রদান করে, পাশাপাশি ডাটা সেন্টার জুড়ে শীতল বাতাসের সর্বাধিক সরবরাহ নিশ্চিত করে। উত্থিত মেঝে একটি উচ্চতর Signal Reference Ground (SRG) সরবরাহ করে, যার মাধ্যমে উল্লেখ্য গ্রিড যান্ত্রিকভাবে মেঝের সাথে সংযুক্ত হয়। উত্থিত মেঝে আধুনিক কম্পিউটার সরঞ্জামগুলির জন্য ঠান্ডা বাতাসের সর্বোত্তম সরবরাহ করে যা সাধারণত নিচ-থেকে-উপরের দিকে বায়ু প্রবাহের জন্য ডিজাইন করা হয়। উপরন্তু, উত্থিত মেঝে বৈদ্যুতিক এবং সংকেত তার ব্যবস্থাপনার জন্য উপযুক্ত পরিবেশ প্রদান করে। RAF এর জন্য মেঝের টালি নির্বাচন করার সময় এটির প্রয়োজনীয় সর্বোচ্চ মেঝের ভারবহন ক্ষমতা নির্ণয় করা গুরুত্বপূর্ণ। নিম্নে উত্থিত মেঝের উচ্চতা সম্পর্কে সুপারিশ করা হলো:

- ৫০০০ বর্গ ফুট পর্যন্ত স্থাপনা ---১৮ ইঞ্চি RAF উচ্চতা; এবং

- ৫০০০ বর্গ ফুট বেশি স্থাপনা --- ২৪ ইঞ্চি RAF উচ্চতা।

৬.৮. অগ্নি সনাক্তকরণ ও নির্বাপন ব্যবস্থা (Fire Detection and Suppression)

একটি ডাটা সেন্টারে বৈদ্যুতিক কারণে সৃষ্ট আগুনের বিশাল ঝুঁকি থাকে, তাই আগুন সনাক্তকরণ এবং নির্বাপন ব্যবস্থা স্থাপন করা জীবন এবং সম্পত্তি সুরক্ষার জন্য গুরুত্বপুর্ণ, পাশাপাশি ডাটা সেন্টারের দ্রুত কর্মক্ষমতা পুনরুদ্ধার নিশ্চিত করার জন্য জরুরি।

অগ্নি সনাক্তকরণ যন্ত্রটি উত্থিত মেঝে, পাশাপাশি ডাটা সেন্টারের সমগ্র ভবন জুড়ে স্থাপন করা উচিত। সনাক্তকারক হিসাবে তাপ এবং ধোঁয়া উভয়ই সনাক্ত করতে পারে এমন যন্ত্র অন্তর্ভুক্ত করা এবং অগ্নি নির্বাপন ব্যবস্থা, স্থানীয় বিপদ ঘন্টা এবং স্থানীয় বা কেন্দ্রীয় পর্যবেক্ষণ কক্ষের সঙ্গে আন্তঃসংযোগ থাকা দরকার। সনাক্তকারকটি আসন্ন বৈদ্যুতিক আগুনের প্রাথমিক সনাক্তকরণ নিশ্চিত করতে বায়ু প্রবাহের পথ অনুযায়ী ডাটা সেন্টারের কক্ষের ছাদ ও উত্থিত মেঝের নিচে বসানো উচিত।

অগ্নি নির্বাপনের জন্য সাম্প্রতিক এবং প্রযুক্তিগতভাবে উন্নত মাধ্যম হলো ক্লিন এজেন্ট অগ্নি নির্বাপন ব্যবস্থা যা "শীতলীকারক নিমজ্জিত তরল (Immersion Cooling Fluid)" ব্যবহার করে, তাই ডাটা সেন্টারগুলিতে এগুলো ব্যবহার করার পরামর্শ দেওয়া হয়।

৬.৯. পানিজনিত ক্ষতি থেকে সুরক্ষা (Water Damage Protection)

ডাটা সেন্টারের পানিজনিত ক্ষতি শুধুমাত্র অগ্নি নির্বাপক জল থেকে নয়, বরং ভাঙ্গা পানির নল, অতিরিক্ত আদ্রতা থেকে জমা হওয়া পানি, বন্যা ও ভবনের ক্ষতির কারণেও ঘটে। তাই পানি ছিটানোর যন্ত্র (sprinkler) ব্যবহার এড়ানোই বাঞ্ছনীয়। জলজনিত ক্ষতি থেকে রক্ষাকারী যন্ত্র স্থাপন করা প্রয়োজন। এক্ষেত্রে মেঝেতে জোন ভিত্তিক আর্দ্রতা সেন্সর রাখা হয় যা কক্ষের আদ্রতা নিরীক্ষণ করে এবং যখন আদ্রতা দেখা গেলে একটি সতর্ক ঘন্টা বাজায়। নিরাপত্তা কর্মকর্তাদের সর্বদা অবগত রাখতে এবং ক্ষতি হলে প্রতিক্রিয়া সময় কমানোর জন্য নজরদারি ক্যামেরা ব্যবহার করা উচিত। সার্ভারের কেবিনেট (Cabinet) এবং কক্ষগুলোতে এই সূক্ষ্ম উপাদানসমুহকে এমনভাবে স্থাপন করার সুপারিশ করা হয় যে, অল্প পরিমাণে পানি জমা হলেও এগুলো যেন ক্ষতিগ্রস্ত না হয়।

৬.১০. নজরদারী ব্যবস্থা (Surveillance Systems)

আগুন এবং পানি থেকে সৃষ্ট হুমকি কেবলমাত্র নির্দিষ্ট সময় ধরে তথ্য প্রযুক্তি অবকাঠামোগুলিকে বিপুল ক্ষতি করার ক্ষমতা রাখে। তাই সর্বদা সার্ভারের কেবিনেটগুলি (Cabinet), কম্পিউটার কক্ষ এবং সম্পূর্ণ ভবনের উপর নজরদারি করা গুরুত্বপূর্ণ, যাতে ক্ষয়ক্ষতির হলে দ্রুত ব্যবস্থা নেয়া যায়। স্বয়ংক্রিয় আইপি (IP) ভিত্তিক অবলোহিত (Infrared) রশ্মিযুক্ত মুখায়বক চিহ্নিত করতে সক্ষম ক্যামেরার সাহায্যে নজরদারি পদ্ধতি ডাটা সেন্টারের জন্য সুপারিশ করা হয় যা এই ধরণের কাজের উপোযোগী; এটি জোন অনুযায়ী তাপমাত্রা, আর্দ্রতা, বিদ্যুৎ সরবরাহ, শিশির বিন্দু এবং ধোঁয়া বিকাশের মতো ডাটা সেন্টারের পরামিতিগুলিতে নজর রাখে এবং একই সময়ে স্বয়ংক্রিয়ভাবে প্রতিরোধের কাজ শুরু করতে পারে (যেমন তাপমাত্রার সীমার মান অতিক্রম করার সময় পাখার গতি বাড়ানো) বা সতর্ক বার্তা পাঠাতে পারে।

৬.১১. আলোকসজ্জা (Lighting)

- LED সিলিং লাইট স্থাপন করতে হবে যা মেঝে থেকে ৮৫ সে.মি. উপরে এবং এর দীপন ক্ষমতা হবে ৩০০ লাক্স (LUX);
- যথাযথ সংখ্যার লাইট ইউ.পি.এস (UPS) দ্বারা এবং বাকিগুলো LDB দ্বারা বিদ্যুৎ সরবরাহ করা হবে;
- আলোকসজ্জা ব্যবস্থা সাধারণ এবং জরুরি পদ্ধতি মিলে গঠিত। বিদ্যুৎ সরবরাহ যখন শক্তিশালী থাকে তখন সাধারণ আলোটি "চালু" থাকবে। কিছু জরুরি আলো বিকল্প ব্যাটারিসহ সরবরাহ করা উচিত;
- ডাটা সেন্টার এলাকায় স্বাভাবিক আলো এবং কয়েকটি জরুরী আলো সরবরাহ করা উচিত;
- আলোকসজ্জা স্থাপত্য, কার্যকরীতা এবং নান্দনিকতার প্রয়োজন অনুসারে নির্বাচন করা উচিত; এবং
- TIA -942 মানদণ্ড অনুসরণ করে সমস্ত আলোকসজ্জা স্থাপন করতে হবে।

৬.১২. বৈদ্যুতিক কাজের নির্দেশিকা (Electrical Work Guidelines)

৬.১২.১. **বৈদ্যুতিক তার (Electrical Cabling) -** বিদ্যমান এবং প্রস্তাবিত উপাদানের বৈদ্যুতিক প্রয়োজনীয়তার চেয়ে অধিক ক্ষমতার অগ্নি প্রতিরোধী তার ব্যবহার করা ভালো। ডাটা সেন্টার সম্প্রসারণের জন্য যথাযথ অবস্থানে অতিরিক্ত পাওয়ার পয়েন্ট স্থাপন করা প্রয়োজন।

৬.১২.২. **তারের গুচ্ছায়ণ (Bunching of Wires) -** তড়িৎবাহী বহির্মুখী ও ফিরতি তার যাতে একই আবরক নলে (conduit) টানা হয়, সেভাবে আবদ্ধ করা উচিত। দুটি ভিন্ন উৎসের থেকে উদ্ভুত তার একই আবরক নলের (conduit) মধ্যে চালানো উচিত নয়।

৬.১২.৩. **পরিবাহী সন্নিবেশন (Drawing of Conductors) - এলুমিনিয়াম বা তামার পরিবাহী তার** একই আবরক নলের (conduit) মধ্যে চালানোর সময় খেয়াল রাখতে হবে যাতে ঘষা না খায় বা কেটে না যায়, কারণ ভবিষ্যতে এতে তার ছিঁড়ে যেতে পারে।

৬.১২.৪. **সংযোগ (Joints) -** সমস্ত সংযুক্তি শুধুমাত্র প্রধান সুইচ, বন্টন বোর্ড, সকেট আউটলেট, আলোর আউটলেট এবং সুইচ বাক্সে তৈরি করতে হবে। কোনো তারের সংযুক্তি আবরক নল (conduit) এবং জংশন বাক্সের ভিতরে করা উচিত নয়। পরিবাহী তার আউটলেট থেকে আউটলেটে অবিচ্ছেদ্দ হওয়া প্রয়োজন।

৬.১২.৫. **প্রধান ও উপপ্রধান তার (Mains and Sub-Mains) -**প্রধান ও উপপ্রধান তার উচ্চ ক্ষমতাযুক্ত এবং অনুমোদিত হওয়া উচিত। প্রতিটি প্রধান এবং উপপ্রধান তার পর্যাপ্ত আকারের নিজস্ব আবরক নলের (conduit) মধ্য দিয়ে টানতে হবে। প্রধান ও উপপ্রধান তার সহজে টানার জন্য সুবিধামত স্থানে পর্যাপ্ত আকারের ড্র বাক্স সরবরাহ করতে হবে। ভূমি সংযোগের জন্য সঠিক রেটিং এর তার ব্যবহার করতে হবে। প্রধান ও উপপ্রধান তারের পাশ দিয়ে ভূমি সংযোগ তার টানতে হবে।

৬.১২.৬. **পরিবাহীর রঙের কোডিং (Color Code of the Conductors) -** পুরো তারের সংযোগে রঙের কোড বজায় রাখতে হবে; তিন ফেজের জন্য লাল, হলুদ, নীল এবং বন্ধ নিরপেক্ষ বর্তনীর জন্য কালো ও ভূমি সংযোগের জন্য সবুজ রঙ ব্যবহার বাঞ্চনীয়।

৬.১২.৭. **তারবাহী আবরক নলের স্থাপন (Fixing of the Conduits) –** তারবাহী আবরক নলের সংযোগ বাক্স অবশ্যই যথাস্থানে হবে এবং শক্ত করে আটকানো থাকবে। নল গুলো এমন ভাবে রাখতে হবে যাতে সহজেই তার লাগানো যায়। অনুমোদিত আকার-আকৃতির সংযোগ বাক্স পর্যাপ্ত পরিমানে থাকতে হবে। সকল তারবাহী আবরক নল বাষ্প ও গরম পানির নল থেকে দূরে স্থাপন করতে হবে। তারবাহী আবরক নল, সংযোগ বাক্স, বহির্মুখী বাক্স এবং স্যুইচ বাক্স বসানো শেষ হবার পর এর ঢাকনা ভালোভাবে বন্ধ করে দিতে হবে যাতে পানি, ধুলাবালি, পোকামাকড় বা অন্য বাইরের বস্তু প্রবেশ করতে না পারে। তারবাহী নল গুলো সুষ্ঠ ও সংগঠিত পদ্ধতিতে স্থাপন করতে হবে যাতে তা অন্যান্য পরিষেবার লাইন বা নলের প্রবাহে বিঘ্ন না ঘটায়।

৬.১২.৮. **সুরক্ষা (Protection) -** পরিবাহীর মধ্যে বাষ্প বা শিশির যাতে জমা না হয় তাই তারবাহী নলে বায়ূ চলাচলের ব্যবস্থা থাকতে হবে। সমস্ত সংযোগ অবশ্যই উপযুক্ত দ্রব্যাদি দ্বারা পানিরোধী করতে হবে।

৬.১২.৯. **সুইচ ও সংযোগ বাক্স (Switch-Outlet Boxes and Junction Boxes) -** সব বাক্স বাংলাদেশের চলতি মানদন্ড অনুযায়ী হবে। আচ্ছাদন ভাল মানের হতে হবে, যা যান্ত্রিকভাবে শক্তিশালী এবং অগ্নিরোধক। প্রয়োজন অনুসারে সুইচগুলির আচ্ছাদন ঠিক করার সুবিধা থাকতে হবে। ভূমি সংযোগের জন্য বাক্সের মধ্যে সংযোগ প্রদান করতে হবে।

৬.১২.১০. **পরিদর্শন বাক্স (Inspection Boxes) -** বাইরে ও ভিতরে মসৃন তলদেশযুক্ত মরিচারোধী বাক্সগুলো নিয়মিত পরিদর্শন এবং প্রয়োজনে তারের অপসারণ ও প্রতিস্থাপন সহজতর করে।

৬.১২.১১. **ভূমি সংযোগকারী তার (Earthing) -** ডাটা সেন্টার জন্য TIA -942 টেলিযোগাযোগ অবকাঠামো মানদন্ড দ্বারা সংজ্ঞায়িত এর সরঞ্জামগুলির মান যথাযথ স্থানাঙ্কের ভিত্তিতে, সাধারণত নেটওয়ার্ক গ্রাউন্ডিং বা ডাটা সেন্টারের গ্রাউন্ডিং অবকাঠামো হিসাবে তামার ফলক এবং ফালা দিয়ে ভূমির সাথে যুক্ত থাকা উচিত। একক স্থানে একত্রে সংযুক্ত সমস্ত ভূমি সংযোগ তারের রোধের যোগফল অবশ্যই ১ ওহম (Ohm) থেকেও কম থাকতে হবে।

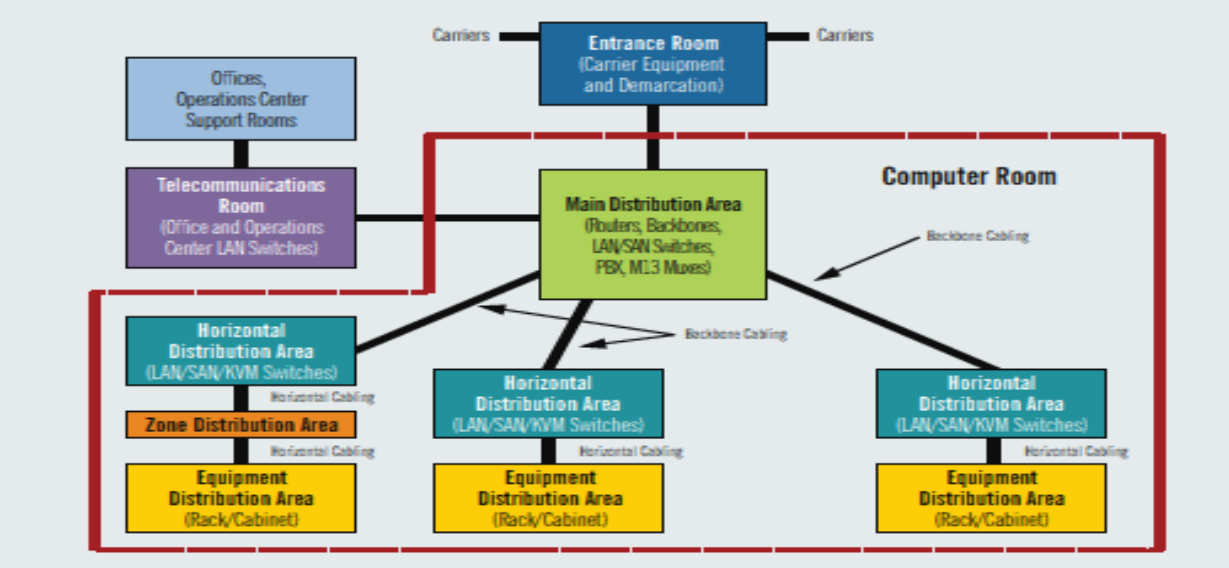
৬.১৩. ইদুর এবং এর বিতারণ ব্যবস্থা (Rodent and Repellent System (RRS)) – শ্রবণাতীত শব্দের ইদুর বিতারণ ব্যবস্থা ডাটা সেন্টারে স্থাপন করা বাঞ্ছনীয়।

৬.১৪. পরিবেশ ও অবকাঠামো ব্যবস্থাপনা (Environment and Infrastructure Management Tools) - ডাটা সেন্টারের পরিবেশ ও অবকাঠামো ব্যবস্থাপনার জন্য সফটওয়ার সরঞ্জাম ব্যবহার করা উচিত।

৭. ডাটা সেন্টারের বিন্যাস (Data Center Layout)

ডাটা সেন্টারের নকশা প্রস্তুত করার সময় অবশ্যই লক্ষ্য রাখতে হবে যেন ডাটা সেন্টারের ভেতরে প্রচুর ফাঁকা জায়গা থাকে, যাতে ভবিষ্যতে চাহিদা অনুসারে পর্যাপ্ত সার্ভার স্থাপন করার জন্য নতুন রাক ও কেবিনেট স্থাপন করা যায়। এছাড়া ডাটা সেন্টারের আশেপাশে পর্যাপ্ত খালি জায়গা রাখতে হবে যাতে ভবিষ্যতে সহজেই ডাটা সেন্টারের সম্প্রসারণ করা সম্ভব হয়।

TIA -942 এর একটি বড় অংশ স্থাপনা সম্পর্কিত। এই মানদন্ড নির্দিষ্ট কার্যকরী এলাকার সুপারিশ করে যা মানসম্মত স্তরীভূত তারকা টোপোলজি (hierarchical star topology) নকশার উপর ভিত্তি করে সরঞ্জামের অবস্থান নির্ধারণ করতে সহায়তা করে। এই কার্যকরী এলাকা বিশিষ্ট একটি ডাটা সেন্টারের নকশা এর ভবিষ্যতের সম্প্রসারণে সহয়তা করে এবং এমন পরিবেশ তৈরি করে যেখানে অ্যাপ্লিকেশন এবং সার্ভারগুলোকে সহজে যুক্ত করা যায় এবং ন্যুনতম ডাউনটাইম এবং ব্যতয়্যের মধ্যে আপগ্রেড করতে সক্ষম। নিচের চিত্রে ডাটা সেন্টারের বিন্যাস দেখানো হল:



৭.১. কার্যকরী এলাকা (Functional Areas)

একটি ডাটা সেন্টারে নিম্নোক্ত কার্যকরী এলাকা থাকা আবশ্যকঃ

প্রবেশ কক্ষ (বাহ্যিক নেটওয়ার্ক ইন্টারফেস) **(Entrance Room (External Network Interface)):** এটি ডাটা সেন্টারে নেটওয়ার্কের প্রবেশ এলাকা যা বাইরের নেটওয়ার্কের (ইন্টারনেট প্রদানকারী) অভিগমণের জন্য বিবেচিত হয় এবং স্তরের (Tier) উপর নির্ভর করে একাধিকভাবে সংযুক্ত থাকতে পারে। ছোট নেটওয়ার্কের ক্ষেত্রে, বাহ্যিক নেটওয়ার্ক ইন্টারফেসটি সরাসরি অনুভূমিক বিতরণ এলাকার (স্থানীয় পরিবেশক) সাথে সংযুক্ত থাকে।

মূল বিতরন এলাকা (প্রধান পরিবেশক) **(Main Distribution Area (Main Distributor))**: এই এলাকাটি ডাটা সেন্টারের মূল অংশকে প্রতিনিধিত্ব করে, এই কারণে শুধুমাত্র এই অঞ্চলে অতিরিক্ত সংযোগ থাকে এবং এর উপাদানগুলি অত্যন্ত গুরুত্বপূর্ণ। ব্যাকবোনে সমস্ত তথ্যের পরিবহন এখানে নিয়ন্ত্রিত হয়, এই কারণে নেটওয়ার্কটির এই অংশটি মূল বিন্যাস (Core Layer) হিসাবে পরিচিত। যাইহোক, সমষ্টি স্তর (বা বিতরণ স্তর), যার বন্টন স্যুইচের সমষ্টি এবং অন্তস্থলের প্রবেশ বিন্যাস যা তথ্য পরিবহন করে, এ স্থানে অবস্থিত।

অনুভূমিক বিতরণ এলাকা (স্থানীয় পরিবেশক) **(Horizontal Distribution Area (Zone Distributor)):** ব্যাকবোন এবং অনুভূমিক ক্যাবলের মধ্যে এই "ইন্টারফেস" এ, অ্যাক্সেসের ডাটা ট্র্যাফিক টার্মিনাল ডিভাইসগুলোর সাথে ডাটা আদানপ্রদান নিয়ন্ত্রণ করে। নেটওয়ার্কের এই এলাকাটি অভিগমন স্তর (Access Layer) হিসাবে পরিচিত।

আঞ্চলিক বিতরন এলাকা (স্থানীয় বিতরণ পয়েন্ট) **(Zone Distribution Area (Local Distribution Point)):** এটি সরঞ্জাম বিতরণ এলাকায় "মধ্যবর্তী বন্টন" করে, যা স্থানীয়ভাবে ব্যবহৃত হয় এবং উত্থিত মেঝেতে রাখা হয়।

দুরালাপনী কক্ষঃ এখানে অভ্যন্তরীণ নেটওয়ার্কের সংযোগ অবস্থিত থাকে।

পরিচালনা কক্ষ, সহায়ক কক্ষ এবং আপিস হল ডাটা সেন্টারে নিযুক্ত কর্মীদের কক্ষ।

৭.২. কক্ষের ধারণা (Room Concept)

ডাটা সেন্টারের বিন্যাস অনুযায়ী বিভিন্ন কক্ষের ধারণা গড়ে উঠেছে। প্রথাগত **কক্ষের মাঝে কক্ষ (Room in Room)** ধারণার সাথে আলাদা প্রযুক্তি ও তথ্য প্রযুক্তি নিরাপত্তা কক্ষ থাকে যেখানে উত্থিত মেঝের উপর যেকোনো সংখ্যক ও ধরণের সার্ভার র‍্যাক এবং নেটওয়ার্ক বাক্স, প্রয়োজনে ঝুলন্ত ছাদ, প্রত্যক্ষ ও পরোক্ষ অগ্নি সুরক্ষা ব্যবস্থা এবং শীতলীকরণ সুবিধা থাকতে পারে।

৮. তথ্য প্রযুক্তি অবকাঠামো (Information Technology (IT) Infrastructure)

৮.১. ক্যাবলিং ব্যবস্থা (Cabling System)

ডাটা সেন্টারে তথ্য প্রযুক্তি সংক্রান্ত অ্যাপ্লিকেশনগুলোকে সর্বদা ব্যবহারোপযোগী রাখার জন্য যোগাযোগে সক্ষম ক্যাবলিং ব্যবস্থা অপরিহার্য। একটি উচ্চ-কর্মক্ষমতা সম্পন্ন ক্যাবলিং সিস্টেম ছাড়া, সার্ভার, সুইচ, রাউটার, স্টোরেজ ডিভাইস এবং অন্যান্য সরঞ্জাম একে অপরের সাথে যোগাযোগ এবং তথ্য বিনিময়, প্রক্রিয়াকরণ এবং সংরক্ষণ করতে পারবে না। ডাটা সেন্টারগুলির জন্য ক্যাবলিং এর আধুনিক শর্তাদি নিম্নরূপ:

- উচ্চ চ্যানেল ঘণত্ব (High channel densities);
- উচ্চগতির ট্রান্সমিশন (High transmission speeds);
- বাধা/বিঘ্নহীন হার্ডওয্যার পরিবর্তন (Interruption-free hardware changes);
- বায়ুচলাচল ব্যবস্থা (Ventilation aspects); এবং
- প্রয়োজনীয় সমর্থন (Support)।

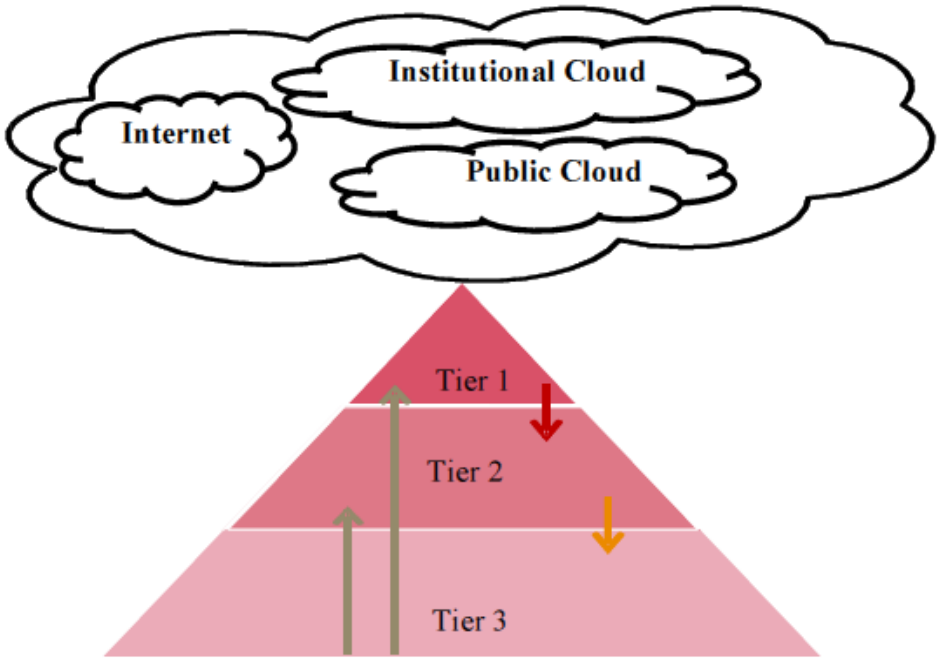
সাবধানতা, দূরদর্শী পরিকল্পনা এবং সুগঠিত ক্যাবলিং ব্যবস্থা তাই ডাটা সেন্টারের পরিচালনাকারীদের দায়িত্বগুলোর মধ্যে উল্যেখযোগ্য। ডাটা সেন্টারের ক্যাবলিং ব্যবস্থা পরিকল্পনা করার সময় নিম্নলিখিত বিষয়গুলি বিবেচনা করা দরকার:

- কোরে অতিরিক্ত (Redundancy) ক্যাবলিং অনাবশ্যক;
- ভবন মধ্যে অতিরিক্ত লিঙ্ক;
- কোরের ব্যান্ডউইথ বৃদ্ধি;
- প্রান্ত বিন্দুতে ব্যান্ডউইথ বৃদ্ধি;
- ভয়েস ওভার আইপি (VoIP) সম্প্রসারণের জন্য QoS নিয়ন্ত্রণ;
- LAN এবং WAN এ ভিডিও স্ট্রিমিং এবং ভিডিও বিতরণের জন্য সম্পূর্ণ সমর্থন;
- VLAN এর মধ্যেকার যোগাযোগে কঠোর নীতিমালা; এবং
- ডাটা সেন্টার থেকে DR সাইটে তথ্য প্রতিলিপি (Replication) করার ব্যবস্থা।

নির্দেশনা (Guideline) - বাণিজ্যিক ভবনে টেলিযোগাযোগ ক্যাবলিং মানদণ্ড অনুযায়ী TIA -568-B.1, TIA -568-B.2, TIA -568-B.3, TIA-569-B, TIA -606-B, বাণিজ্যিক ভবনগুলোর টেলিযোগাযোগ অবকাঠামোর জন্য প্রশাসনিক মান TIA-606-A, টেলিযোগাযোগের জন্য বাণিজ্যিক ভবনের গ্রাউন্ডিং এবং বন্ডিং শর্ত TIA -607 মান অনুযায়ী ডাটা সেন্টারের জন্য কাঠামোগত ক্যাবলিং সিস্টেম (SCS) বিবেচনা করা উচিত।

৮.২. নেটওয়ার্ক (Network)

একটি ডাটা সেন্টারের নেটওয়ার্ক প্রতিষ্ঠার জন্য কোনো আদর্শ নির্দেশিকা নেই। তবে ক্লাউড কম্পিউটিং, ওয়েব ভিত্তিক অ্যাপ্লিকেশন এবং নিরাপত্তা দিক সাম্প্রতিক প্রবণতা বিবেচনা করে, একটি পৃথক নেটওয়ার্ক মডেলের সুপারিশ করা হয়। নীচের চিত্রে প্রস্তাবিত তিন-স্তর বিশিষ্ট নেটওয়ার্ক মডেল দেখায়:



উপরের মডেলের প্রতিটি স্তর পৃথক ফায়ারওয়ালের মাধ্যমে আলাদা করা হয়। কম নির্ভরযোগ্য স্তরে উত্থাপিত যোগাযোগগুলি শুধুমাত্র পরবর্তী নিচের স্তরে প্রবেশ করতে পারে (প্রথম স্তর সবচেয়ে কম নির্ভরযোগ্য এবং তৃতীয় স্তরটি সবচেয়ে নির্ভরযোগ্য)। স্তরগুলোর মধ্যে বিচ্ছিন্নতা এবং ফায়ারওয়াল সীমাবদ্ধতার সমন্বয়ে নিম্ন স্তরে নির্ভরযোগ্যতার ক্রমবর্ধমান স্তর অনুযায়ী একই সময় একটি মাত্র স্তরের সাথে যোগাযোগের অনুমতি দেয়া হয়। মডেলের প্রতিটি স্তর নির্দিষ্ট কিছু কাজ সম্পন্ন করে, যেমন সার্ভারের লোড ভারসাম্য, স্থিতিস্থাপকতা এবং মূল উপাদানগুলির উচ্চতর প্রাপ্যতা।

৮.২.১. নেটওয়ার্ক পৃথকীকরণ (Network Segregation)

ওয়েব, অ্যাপ্লিকেশন এবং ডাটা জোন ৩ টি পৃথক স্তরের মধ্যে হোস্ট করা উচিত। এই নকশাটি ফায়ারওয়াল / রাউটিং যন্ত্রের দ্বারা স্তরটির মধ্যে এবং বাইরে নিয়ন্ত্রণ বজায় রাখে এবং কোনো সার্ভার একে অপরের সাথে যোগাযোগ করতে পারে তা নির্ধারন করে।

- **প্রথম স্তর – অনির্ভরযোগ্য স্তর (Tier 1 – Untrusted layer)**
  প্রথম স্তর (Tier 1) বাইরের বিশ্বের (সাধারণ জনসাধারণের) কাছে ওয়েব পরিষেবা সরবরাহ করতে ব্যবহৃত হয়। প্রথম স্তর (Tier 1) একটি বাহ্যিক ফায়ারওয়ালের মাধ্যমে ফিল্টার করা হয় এবং অন্যান্য স্তরে পরবর্তী ট্র্যাফিক একটি অভ্যন্তরীণ ফায়ারওয়ালের মাধ্যমে পাঠানো হয়। সুরক্ষা বাড়ানোর জন্য প্রথম স্তরকে (Tier 1) বিভিন্ন অঞ্চলে ভাগ করা হয় (উদাহরণ: ওয়েব পরিষেবাসমূহ এবং ইন্টারনেটের মাধ্যমে প্রদত্ত ওয়েব পরিষেবাদিতে প্রবেশের পরিষেবা)।
- **দ্বিতীয় স্তর – অল্পনির্ভরযোগ্যযোগ্য স্তর (Tier 2 – Semi-trusted layer)**
  দ্বিতীয় স্তর (Tier 2) উপস্থাপনা (Presentation) সার্ভারগুলোর ডাটার জন্য অনুরোধগুলি পর্যালোচনা করে এবং ডাটাবেস সার্ভার থেকে এই ডাটাটি পুনরুদ্ধার করে। এই স্তর সেই ডাটায় বিভিন্ন প্রক্রিয়াকরণ ফাংশন প্রয়োগ করে এবং ফলাফলগুলিকে প্রথম স্তরের (Tier 1) ডিভাইসে পাঠায়। প্রথম স্তরে সমস্ত প্রক্রিয়াকরণের অনুরোধ (Processing Request) দ্বিতীয় স্তরে (Tier 2) পৌঁছানোর আগে একটি অভ্যন্তরীণ ফায়ারওয়ালের মধ্য দিয়ে যাবে। দ্বিতীয় স্তরে (Tier 2) সার্ভার হোস্ট করার জন্য বিভিন্ন অঞ্চলে পৃথক করা যায়।
- **তৃতীয় স্তর – নির্ভরযোগ্য স্তর (Tier 3 – Trusted layer)**

তৃতীয় স্তর (Tier 3) অ্যাপ্লিকেশন ডাটা সংরক্ষণ করে। এই স্তর নেটওয়ার্কের সবচেয়ে নিরাপদ এবং যৌক্তিকভাবে (Logically) বিচ্ছিন্ন এলাকা যেখানে তথ্য সংরক্ষণকারী ডাটাবেস সার্ভার হোস্ট করা হয়। এই স্তরের ডাটা দিত্বীয় স্তরের উপর অনির্ভরশীল। দ্বিতীয় স্তর (Tier 2) থেকে তৃতীয় স্তর (Tier 3)এর অনুরোধগুলি পৌঁছানোর আগে অভ্যন্তরীণ ফায়ারওয়ালের মধ্য দিয়ে যেতে হবে। তৃতীয় স্তর (Tier 3) অভ্যন্তরীণ এবং বাইরের সার্ভারকে হোস্ট করার জন্য একাধিক অঞ্চলে পৃথক করা যেতে পারে। (উদাহরণ: ডাটাবেস সার্ভার যেগুলো অন্যান্য সংস্থার অনুরোধ গ্রহণ করে এবং যেগুলো শুধুমাত্র অভ্যন্তরীণ ল্যান থেকে অনুরোধ গ্রহণ করে)।

৮.২.২. নির্দেশিকা প্রণয়নের নীতিমালা (Guiding principles)

- **নিরাপত্তা (Security) –** ডাটা সেন্টার নেটওয়ার্ক স্থাপত্যে (architecture) তথ্য গোপনীয়তা (Confidentiality), সত্যতা (authenticity) এবং বিশুদ্ধতা (integrity) নিশ্চিত করা উচিত। তথ্য বিনিময় নির্ভরযোগ্য হওয়া উচিত যা প্রতিষ্ঠিত নিরাপত্তা নীতির সাথে সঙ্গতিপূর্ণ, যেখানে তথ্যের অননুমোদিত অধিকরণ (Access), পরিষেবা অস্বীকার এবং ইচ্ছাকৃত / আকস্মিক পরিবর্তনের বিরুদ্ধে সুরক্ষা বিদ্যমান।
- **প্রাপ্যতা (Availability) –** উচ্চ প্রাপ্যতার জন্য নেটওয়ার্ক উপাদানগুলি নির্ভরযোগ্য হওয়া উচিত এবং এতে পরিষেবা স্তরে চুক্তির (SLA) সুস্পষ্ট উল্লেখ থাকে কিন্তু নেটওয়ার্কের স্থাপত্যে (Architecture) অতিরিক্ত উপাদান থাকে যাতে কোনো ব্যর্থতার একক বিন্দু (Single Point of Failure) না থাকে।
- **কার্যক্ষমতা ও সম্প্রসারণযোগ্যতা (Performance and Scalability) -** নেটওয়ার্ক ব্যবস্থায় গ্রহণযোগ্য প্রতিক্রিয়া করার সময় থাকা উচিত এবং অবকাঠামোটিতে অতিরিক্ত ব্যান্ডউইথ এবং নিকট ভবিষ্যতে নতুন ব্যবহারকারীর সেবা দেবার জন্য নেটওয়ার্কটি সম্প্রসারণযোগ্য হওয়া উচিত।
- **নমনীয়তা (Flexibility) –** নেটওয়ার্ক ব্যবস্থার উপাদানগুলি পরিকল্পিত খরচের মধ্যে পরিবহন, পরিবর্তন, পরিবর্ধন ও সংযোজনযোগ্য হবে।

৮.৩. সার্ভার (Servers)

সার্ভার নির্বাচন করার জন্য সুনির্দিষ্ট কোনো মানদন্ড নেই। একটি সার্ভারের প্রযুক্তিগত বৈশিষ্ট্য নির্ধারণ করা হয়, সাধারণত সার্ভারে চলমান অ্যাপ্লিকেশনের প্রক্রিয়াকরণ ক্ষমতা (Processing Power), প্রতিক্রিয়ার সময় (Response Time), মেমরি ক্ষমতা, হার্ড ডিস্কের ক্ষমতা ইত্যাদি বিষয়ের উপর নির্ভর করে। তাই উপযুক্ত কনফিগারেশনে নিরাপদ, নির্ভরযোগ্য, দক্ষ, সম্প্রসারণযোগ্য (Scalable) এবং সহজে রক্ষণাবেক্ষণযোগ্য সঠিক সার্ভার নির্বাচন করা খুবই গুরুত্বপূর্ণ।

৮.৩.১. মূল বিবেচ্য বিষয় (Key Considerations)

সার্ভার বেছে নেওয়ার ক্ষেত্রে নিচের বিষয়গুলো বিবেচনা উচিতঃ

- আপনার প্রথম বিবেচ্য বিষয় হল সার্ভারের কার্যকারিতা। স্পষ্টতই আপনি এমন কোনো সার্ভার বিবেচনা করবেন না যা আপনার সংস্থার প্রয়োজনীয়তা পূরণ করতে পারবে না;
- আপনার প্রতিষ্ঠানের জন্য সঠিক মূল্যে এমন সার্ভার নির্বাচন যাতে অপ্রয়োজনীয় কিছুর জন্য আপনি অর্থ ব্যয় করবেন না;
- আপনি আগেই চিন্তা করুন, সার্ভার ভাড়া (Rent) নিবেন, নাকি কিনবেন। দুশ্চিন্তা এড়ানোর জন্য স্বল্প মেয়াদে সার্ভার ভাড়া করা একটি সঠিক সিদ্ধান্ত হতে পারে, তবে এই সিদ্ধান্ত আপনার কার্যক্ষমতাকে বড়ই সীমিত করে ফেলতে পারে। প্রয়োজন হলে কার্যকারিতা নিয়ে আরেকবার চিন্তা করুন;
- প্রয়োজন অনুযায়ী হার্ডওয়ার বুঝে নিন। আপনি যদি কিনতে চান, তবে আপনাকে অবশ্যই নিজস্ব সার্ভারের জন্য হিসাব করতে হবে। আপনার বর্তমান অবকাঠামো আপনার সার্ভারগুলিকে সুষ্ঠুভাবে পরিচালনা করতে সক্ষম হবে কিনা তা নির্ধারণের জন্য এবং সেই একই অবকাঠামো প্রতিষ্ঠানের প্রবৃদ্ধিকে/সম্প্রসারনকে সমর্থন করতে পারে

কিনা তা নির্ণয়ের জন্য আপনি দায়বদ্ধ হবেন। এখন অনেক ব্যবসায় সার্ভার ভার্চুয়ালাইজেশন (VPS) এবং অত্যাধুনিক ক্লাউড-ভিত্তিক সার্ভারে চালু হচ্ছে কারণ সেগুলো বাহ্যিক হার্ডওয়ারের উপর নির্ভরতা ছাড়াই পর্যাপ্ত কর্মক্ষমতা দেখাতে সক্ষম;

- আপনার সার্ভারে প্রয়োজন হতে পারে এমন যে কোনো অতিরিক্ত সফটওয়্যার সম্পর্কে জেনে নিন। সফটওয়্যার সম্পর্কে প্রধান বিবেচ্য বিষয়ের একটি হল, আপনি উইন্ডোজ বা লিনাক্স অপারেটিং সিস্টেম ব্যবহার করে সার্ভার চালাতে চান কিনা। অতএব, ক্রয় করার আগে আপনার প্রয়োজনীয় সবকিছু সম্পর্কে খোঁজ নিন এবং আপনার মোট খরচ নির্ণয় করুন। সার্ভার ব্যয়বহুল হতে হবে এমন নয়, তবে আপনি সেগুলো কীভাবে ব্যবহার করছেন তার উপর নির্ভর করে খরচ অনেক বৃদ্ধি পেতে পারে;
- প্রতিষ্ঠানের সকল নতুন হার্ডওয়ার এবং সফটওয়্যার বিদ্যমান সার্ভারে সংযুক্ত করার বিষয়েও ভাবতে হবে। আপনার যদি ইতিমধ্যে কোনো সার্ভার বা নেটওয়ার্ক থাকে, তবে নতুন কোনো ক্রয়, অবশ্যই ইতিমধ্যে যা আছে তা সম্প্রসারণের জন্য করতে হবে;
- হার্ডওয়ার এবং সফ্টওয়ার উভয়ই হিসাবের সময়, আপনি চলমান ব্যবস্থার রক্ষণাবেক্ষণের হিসাবও বিবেচনা করুন। কোনো সার্ভারকে কার্যকরী রাখতে, পরিকল্পিত ডাউনটাইম সহ আপনার প্রতিষ্ঠানের জন্য কোনো সার্ভারটি সঠিক, সেটা বিবেচনায় নিয়ে সিদ্ধান্ত নেওয়ার একটি গুরুত্বপূর্ণ অংশ;
- প্রথমতঃ তথ্য সুরক্ষার জন্য একটি প্রতিষ্ঠান সার্ভার ব্যবহার করে । আপনি কী সুরক্ষিত রাখতে চান এবং আপনি কীভাবে এটি করতে যাচ্ছেন তা নিয়ে ভাবুন;
- কোনো সার্ভারের উপযুক্ততা নির্ধারণ করার সময় এর সম্প্রসারণযোগ্যতা (Scalability) অত্যন্ত গুরুত্বপূর্ণ। প্রতিষ্ঠানকে সর্বদা সম্প্রসারণযোগ্য সার্ভার নির্বাচন করা উচিত; এবং
- একটি সার্ভার কেনার সময় চূড়ান্ত এবং সম্ভবত সবচেয়ে গুরুত্বপূর্ণ বিষয় হল, সেটা আপনার ব্যবসার জন্য সহায়ক একটি সেবা। কোনো সার্ভার থেকে সর্বাধিক সেবা পেতে, প্রতিষ্ঠানকে মাঝেমাঝে প্রযুক্তিগত সহায়তার উপর নির্ভর করতে হতে পারে। বিভিন্ন সার্ভার কোম্পানির সহায়তা সেবা সম্পর্কে হোস্টিং ফোরামে গ্রাহকদের সমালোচনাগুলো বিস্তারিত পড়ুন। এটি সিদ্ধান্ত নেওয়ার প্রক্রিয়ায় একটি বড় সহায়ক হতে পারে।

৮.৪. তথ্য সংরক্ষণ (Storage)

একটি তথ্য সংরক্ষণাগার (Storage) নির্বাচন করার জন্য কোনো আদর্শ মানদণ্ড নেই। একটি তথ্য সংরক্ষণাগার (Storage) নির্বাচন, একটি প্রতিষ্ঠানের তথ্যের আকার ও প্রবৃদ্ধি, তথ্যের ব্যাকআপ (Backup) এবং সংরক্ষণের প্রয়োজনীয়তার উপর নির্ভর করে।

তথ্য সংরক্ষণাগার (Storage) একটি জটিল বিষয়। কোনো প্রতিষ্ঠানের তথ্য সংরক্ষণাগার (Storage) নির্বাচন কঠিন, কারণ এটি প্রায়শই সর্বোত্তম লাভ পাওয়ার জন্য বেশী দামি যন্ত্র (Equipment) অন্তর্ভুক্ত করা হয়। প্রতিষ্ঠানের অধিকাংশ নির্বাহীই তথ্য সংরক্ষণ করার প্রয়োজনীয়তা উপলব্ধি করে, তবে তারা এর কর্মক্ষমতা, অধিগম্যতা, প্রাচুর্যতা (Redundancy) ও ঝুঁকি গণনা, বিকল্পতা ও দুর্যোগ পরবর্তী পুনরুদ্ধার সম্পর্কে কমই বিবেচনা করে। সেজন্য তথ্য প্রযুক্তির কাজকে জটিল করে, কারণ প্রতিষ্ঠানের শীর্ষ ব্যবস্থাপকদের কাছে অদৃশ্য এ ব্যবস্থাপনার জন্য কেন বড় বাজেটের দরকার, সেটা ব্যাখ্যা করার প্রয়োজন পড়ে।

তথ্য সংরক্ষণের জন্য অধুনা স্টোরেজ এরিয়া নেটওয়ার্ক (SAN) এবং ব্যাকআপের জন্য টেপ লাইব্রেরি অথবা ডিস্ক ভিত্তিক তথ্য সংরক্ষণাগার ব্যবহৃত হয়।

৮.৪.১. মূল বিবেচ্য বিষয়াদি (Key Considerations):

স্টোরেজ কেনার সময় তিনটি প্রধান বিবেচ্য বিষয় রয়েছে: কার্যক্রম (কীভাবে স্টোরেজ ব্যবহার করা হবে এবং অভিগমন করা হবে), ক্ষমতা ও গতি এবং নির্ভরযোগ্যতা।

- **কার্যক্রম (Function):** স্টোরেজ কেনার অনেক কারণ আছে। কয়েকটি উল্লেখযোগ্য বিষয় হলঃ পৃথক সার্ভার বা ডেস্কটপে স্থানীয়ভাবে বৃহৎ পরিমাণে তথ্য সঞ্চয়স্থান, তথ্য ব্যবস্থাপনাকে কেন্দ্রীভূতকরণ, কর্মক্ষমতা বৃদ্ধি এবং পদ্ধতিগত ব্যর্থতার ক্ষেত্রে তথ্যকে আরও বেশি সহজলভ্য করা। আপনি যদি স্টোরেজটির ফাংশনটি নির্ধারণ করতে না পারেন, তবে আপনার স্টোরেজের প্রয়োজন নেই।
- **ধারণক্ষমতা ও গতি (Capacity & Speed):** ধারণক্ষমতা স্টোরেজের সবচেয়ে সহজ এবং সবচেয়ে স্পষ্ট ফাংশন। কার্যক্ষমতা বা গতি বর্ণনা ও ব্যাখ্যা করা সহজ কিন্তু IOPS হিসাবে পরিমাপ করা আরো কঠিন। IOPS বিভিন্ন ভাবে বর্ণিত হয় যেমন হঠাৎ অভিগমন, ক্রমিক অভিগমন, বিস্ফোরিত গতি, বিলম্ব এবং স্থিতি হারের আশঙ্কা থাকে এবং তারপরে পড়ার এবং লেখার (Read and Write) মধ্যে পার্থক্য। এমনকি ডিভাইসের প্রত্যাশিত পারফরম্যান্সের জন্য প্রয়োজনীয় কর্মক্ষমতা নির্ধারণ করাও কঠিন। কিন্তু সাবধানে গবেষণা করলে এটি অর্জনযোগ্য এবং পরিমাপযোগ্য।
- **নির্ভরযোগ্যতা (**Reliability**):** মনে রাখতে হবে যে, স্টোরেজ "কেবল একটি সার্ভার মাত্র" এবং সাধারণ সার্ভারের ক্ষেত্রে প্রযোজ্য অতিরিক্ততা এবং নির্ভরযোগ্যতার বিষয়গুলি, অংশীদারী স্টোরেজ সিস্টেমের ক্ষেত্রেও সমানভাবে প্রযোগ করা উচিত। প্রায় ক্ষেত্রে, এন্টারপ্রাইজ স্টোরেজ সিস্টেমগুলি এন্টারপ্রাইজ সার্ভারগুলিতে তৈরি করা হয় - একই বাহ্যিক কাঠামো (Chassis), একই ড্রাইভ এবং একই উপাদান। কারণ, নির্ভরযোগ্যতার একই নীতি প্রযোজ্য হবে এবং আপনার জন্য কোনো সরঞ্জাম সঠিক কিনা তা নির্ধারণ করার জন্য আপনাকে অবশ্যই (যেমন থাকা উচিত) একই ঝুঁকি বিবেচনায় নিতে হবে।

মূল্যায়ন, গবেষণা এবং সংগ্রহস্থলের প্রয়োজনীয়তা বিবেচনায় সময় দেয়া করা অত্যন্ত গুরুত্বপূর্ণ কারণ আপনার স্টোরেজ সিস্টেমটি উচ্চ ব্যয় এবং জটিলতার কারণে সম্ভবত দীর্ঘ সময় আপনার নেটওয়ার্কে একটি ব্যাকবোন উপাদান হিসাবে থাকবে। সুতরাং সাবধানে এটি নির্বাচন করুন এবং আপনার মেধা ব্যবহার করুন।

৮.৫. তথ্য নিরাপত্তা (Information Security)

ডাটা সেন্টার এমন একটি স্থান যেখানে তথ্য সংরক্ষণ, প্রক্রিয়াকরণ এবং বিতরণ করা হয়। ডাটা সেন্টারে অবশ্যই গোপনীয়তা (Confidentiality), সত্যতা (Authenticity) এবং বিশুদ্ধতা (Integrity) নিশ্চিত করতে হবে। তথ্য নিরাপত্তা বলতে বোঝায় সরঞ্জাম, নীতি, নিরাপত্তা ধারণা, নিরাপত্তা সুরক্ষা, নির্দেশিকা, ঝুঁকি ব্যবস্থাপনা পদ্ধতি, কর্ম, প্রশিক্ষণ, সর্বোত্তম অনুশীলন (Best Practice), আশ্বাস এবং প্রযুক্তির সংগ্রহ যা ডাটা সেন্টারের পরিবেশ এবং তার সম্পদের সুরক্ষার জন্য ব্যবহার করা যেতে পারে। ডাটা সেন্টারের সাথে সংযুক্ত কম্পিউটিং ডিভাইস, স্টোরেজ ডিভাইস, কর্মচারী, অবকাঠামো, অ্যাপ্লিকেশন, পরিষেবাদি, টেলিযোগাযোগ ব্যবস্থা এবং এতে প্রেরিত এবং / বা সংরক্ষিত তথ্যের সমগ্রতা অন্তর্ভুক্ত। তথ্য নিরাপত্তা সাইবার পরিবেশে নিরাপত্তা ঝুঁকি থেকে ডাটা সেন্টারকে রক্ষা করার চেষ্টা করে।

এই নির্দেশিকার উপ-ধারা ৪.২ এ বর্ণিত তথ্য নিরাপত্তা সম্পর্কিত মানদন্ডসমুহ রয়েছে, যা ডাটা সেন্টারে গ্রহণ করার পরামর্শ দেওয়া হয়। তবে ডাটা সেন্টার সুরক্ষা আর্কিটেকচার সম্পর্কিত বা নিরাপত্তা সম্পর্কিত সরঞ্জাম নির্বাচন করার জন্য কোনো নির্দিষ্ট মানদন্ড নেই।

তবে, তথ্য নিরাপত্তা একটি গুরুত্বপূর্ণ সমস্যা এবং চ্যালেঞ্জ বিবেচনা করে, তথ্য কেন্দ্র এবং তার সম্পদের সর্বোত্তম স্তরের নিরাপত্তা পৌঁছানোর লক্ষ্যে "নিগূঢ় প্রতিরক্ষা (Defense-in-Depth)" পদ্ধতি বাস্তবায়ন করার পরামর্শ দেওয়া হল।

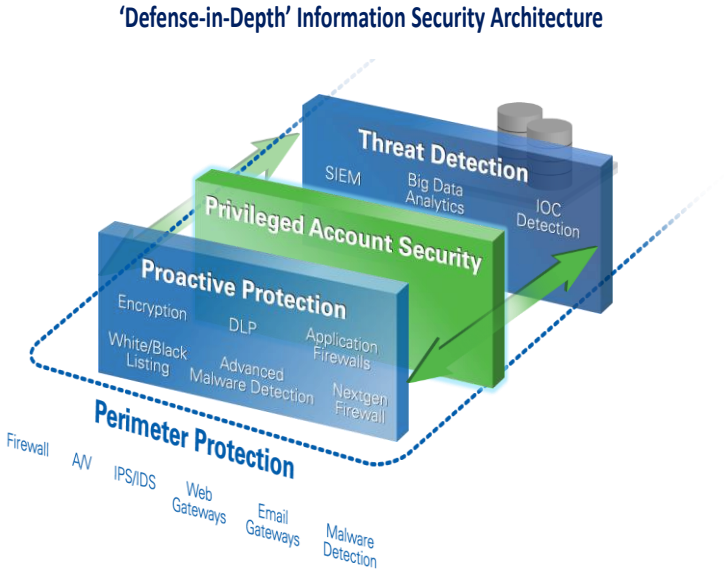
৮.৫.১. তথ্য নিরাপত্তায় 'নিগুঢ় প্রতিরক্ষা' ('Defense-in-Depth' Approach to Information Security)

"নিগূঢ় প্রতিরক্ষা (Defense-in-Depth)" ধারণাটি সামরিক প্রতিরক্ষা থেকে গৃহীত হয়েছে যেখানে আক্রমণকারীকে তার সমস্ত ক্ষমতা প্রয়োগ করতে বাধ্য করার জন্য পদেপদে বাধা স্থাপন করা হয়। তথ্য নিরাপত্তার ক্ষেত্রে, প্রশাসক (Administrator) বা সংস্থা অননুমোদিত অভিগমন (Unauthorized Access) বা তথ্য আক্রমণের ঝুঁকি কমানোর জন্য একাধিক স্তরের প্রতিরক্ষামূলক ব্যবস্থা নেওয়া হয়। সমাপতিত স্তরগুলো দ্বারা অন্য স্তরের দুর্বলতা দূর করা হয়। একটি

সুসংজ্ঞায়িত এবং সুষ্ঠুভাবে প্রয়োগ করা "নিগূঢ় প্রতিরক্ষা" কৌশল বিভিন্ন ধরণের আক্রমণ প্রতিরোধ করে এবং এর প্রশাসকদের কাছে তাৎক্ষণিক অনুপ্রবেশের অ্যালার্মও পেশ করে।

"নিগূঢ় প্রতিরক্ষা" এমন একটি কার্যকর পদ্ধতি, যা স্বয়ংক্রিয়ভাবে হামলা ও আক্রমণের প্রতিরোধ ব্যবস্থা, যা পাবলিক ইন্টারনেট থেকে সৃস্টি হয়। এই ধরনের আক্রমণে, আক্রমণকারী বিভিন্ন পদ্ধতির সাথে চলতি পরিবেশে তথ্য সিস্টেম বা সম্পদের কাজে লাগানোর চেষ্টা করে যা প্রতিরোধ করা অত্যন্ত কঠিন, "নিগূঢ় প্রতিরক্ষা" স্থাপত্যটি ন্যুনতম সুরক্ষা সরবরাহ করতে পারে।

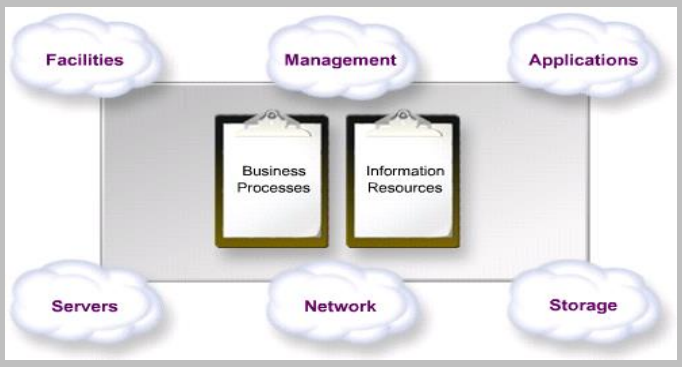
অসামরিকীকৃত এলাকা (Demilitarized Zone (DMZ)), ফায়ারওয়াল, ই-মেইল সিকিউরিটি গেটওয়ে, ওয়েব ফিল্টার, এন্ডপয়েন্ট সুরক্ষা, অনধিকার প্রবেশ প্রতিরোধ ব্যবস্থা (Intrusion Prevention System (IPS)), ম্যালওয়ার সুরক্ষা, ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN), নেটওয়ার্কের আচরণ বিশ্লেষণ, নিরাপত্তা তথ্য এবং ইভেন্ট ম্যানেজমেন্ট সিস্টেম (যেমন: SIEM), ওয়েব এপ্লিকেশন ফায়ারওয়াল (WAF), এন্টি এপিটি, এন্টি-র‍্যান্সোমওয়ার, এন্টি-ডিডিওস, ডিএনএস সিকিউরিটি, ডেটা লস প্রোটেকশন (DLP), সাইবার থ্রেট ইন্টেলিজেন্স (CTI) ইত্যাদি "নিগূঢ় প্রতিরক্ষা" কৌশল সরবরাহ করে তথ্য সুরক্ষার উদ্দেশ্যে ইন্টারনেট বা পাবলিক নেটওয়ার্ক প্রতিষ্ঠানের তথ্য প্রযুক্তির সম্পদকে আক্রমনকারীদের অননুমোদিত অভিগমন অর্জনের লক্ষ্যকে ব্যাহত করে। এসব যন্ত্রের প্রত্যেকটিই আক্রমণকারীদের জন্য বাধা হিসাবে কাজ করে। "নিগূঢ় প্রতিরক্ষা" সংস্থার তথ্য এবং এর সংশ্লিষ্ট প্রযুক্তি আক্রমণকারীদের এবং অনুপ্রবেশকারীদের থেকে রক্ষা করার জন্য একটি যাচাইকৃত (Verified) পদ্ধতি। এই পদ্ধতি এতই নমনীয় (Flexible) যে, এটি সহজেই নতুন উদ্ভূত হুমকির (Arised Threat) বিরুদ্ধে সুরক্ষা প্রদান করতে পারে। নিচের চিত্রে একটি "নিগূঢ় প্রতিরক্ষা" ব্যবস্থার তথ্য সুরক্ষা স্থাপত্যকে নির্দেশ করে:



৯. জনশক্তি (Human Resource)

কার্যত, একটি ডাটা সেন্টারে বিভিন্ন ধরনের সম্পদ রয়েছে, উদাহরণতঃ এর বাহ্যিক স্থাপনা, যেমন সুরক্ষিত সার্ভার কক্ষ, ক্যাবলিং অবকাঠামো, বিদ্যুৎ ও শীতলীকরণ এবং নিরাপত্তা ব্যবস্থা; সার্ভার নেটওয়ার্ক সুবিধা; তথ্য সংরক্ষণ যন্ত্র এবং নেটওয়ার্ক; অ্যাপ্লিকেশন যেমনঃ ব্যবসায় অ্যাপ্লিকেশন এবং ব্যবস্থাপনা অ্যাপ্লিকেশন ইত্যাদি। তবে, মানব সম্পদকে ডাটা সেন্টারের সবচেয়ে গুরুত্বপূর্ণ এবং মূল্যবান সম্পদ হিসাবে বিবেচনা করা হয়।

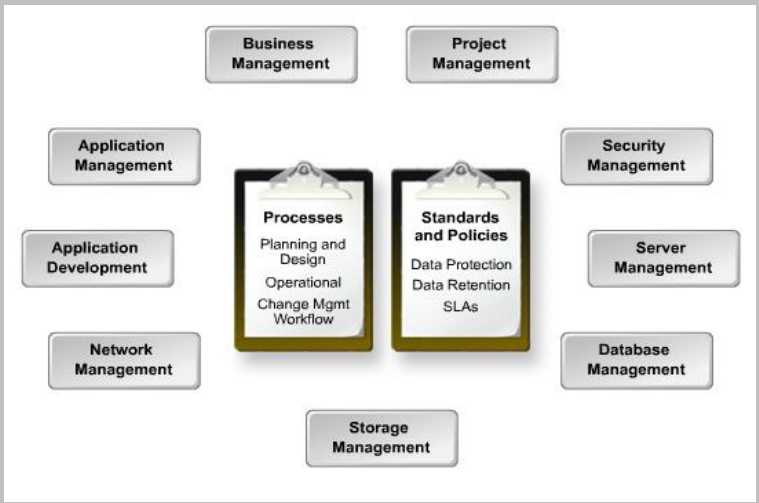
Data Center Resources



All of these resources revolve around management, and maintenance of business processes and information resources

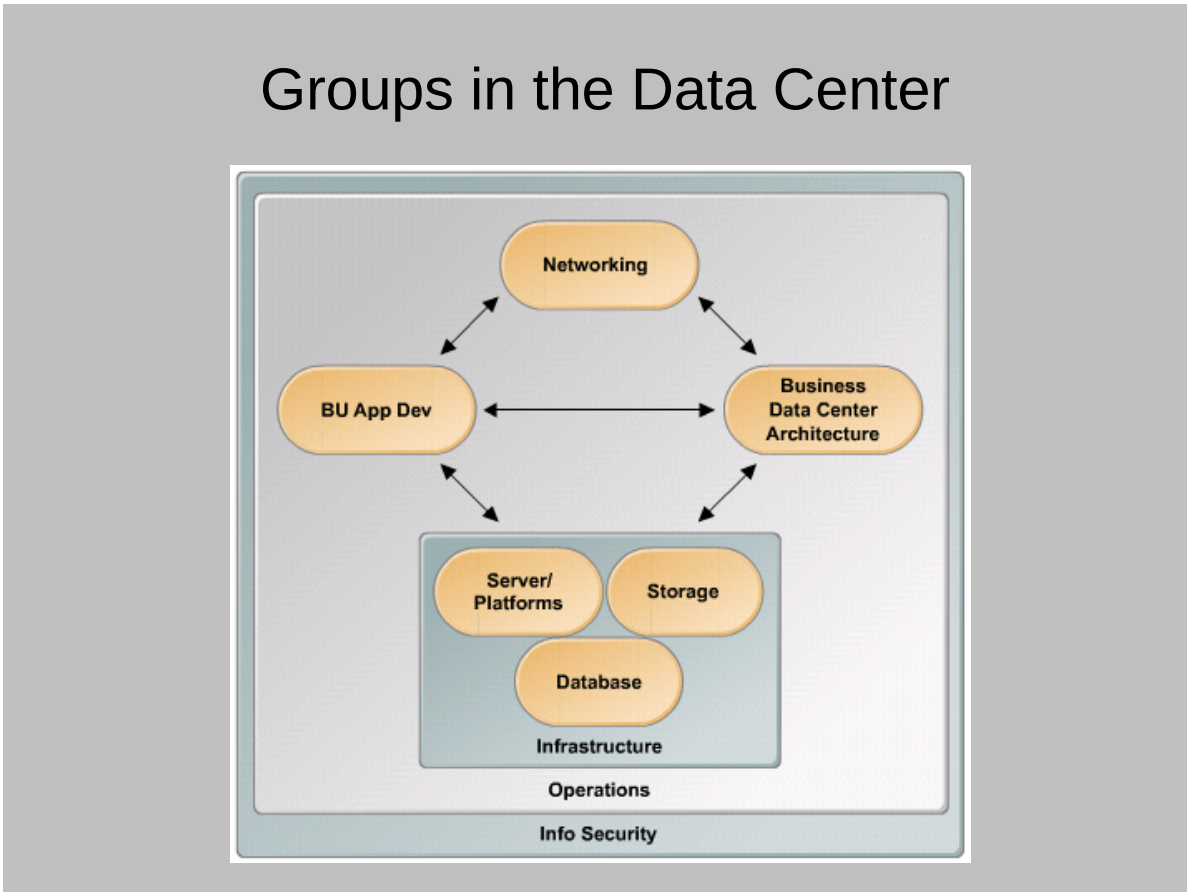
নেটওয়ার্ক স্থাপনার বিপরীতে, ডাটা সেন্টারে একাউন্ট নিয়ন্ত্রণের জন্য বিভিন্ন গোষ্ঠীর মধ্যে সম্পর্ক গড়ে তুলতে হবে। এন্টারপ্রাইজ সেবাপ্রদানকারীর জন্য এই কার্যকরী গোষ্ঠীর সাথে পারস্পরিক যোগাযোগ ছাড়া ডাটা সেন্টারে সফল ভাবে কাজ করা অত্যন্ত কঠিন।

Cross-functional Relationships



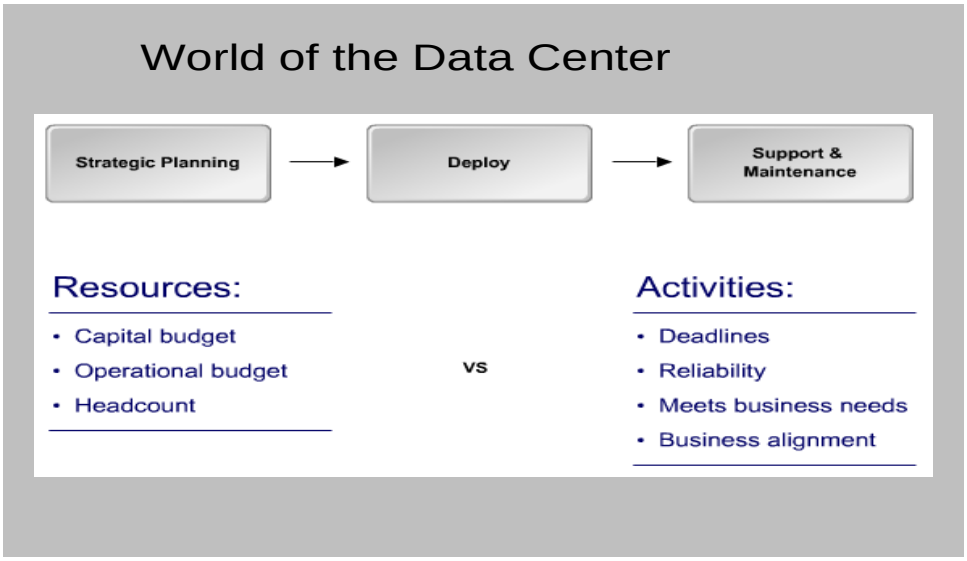
ডাটা সেন্টারের কার্যক্রম এবং উপাদানসমুহ পরীক্ষা করে এবার এর মূল কার্যকরী উপাদানের দিকে নজর দেয়া যাক। এই উদাহরণে ডাটা সেন্টারের বিভিন্ন গোষ্ঠী একসাথে কীভাবে কাজ করে তা ব্যাখ্যা করে। ডাটা সেন্টারে ব্যবসায় ও বিপনন এবং স্থপতি গোষ্ঠী রয়েছে যা উৎপাদনশীলতা, চটজলদিতা এবং স্থিতিশীলতার মতো ব্যবসায়িক লক্ষ্যগুলো নিয়ন্ত্রণ করে। এই বিষয়গুলো তথ্য কেন্দ্র বিকাশের জন্য উদ্যোগ গ্রহণ করে। ডাটা সেন্টার সংস্থা উদ্যোগ বাস্তবায়নের জন্য অবকাঠামো নির্মানকারীদের সাথে কাজ করে। অবকাঠামো প্রকৌশলীরা মানসম্মত পরিবেশ তৈরির জন্য একসঙ্গে কাজ করেন।

নেটওয়ার্ক গ্রুপ (NOC) মানদন্ড এবং পরিবেশ সংজ্ঞায়নে অংশগ্রহণ করে, তবে নেটওয়ার্ক এবং অন্যান্য প্রকৌশল গোষ্ঠীর মাঝে পারস্পারিক যোগাযোগ কম থাকে।



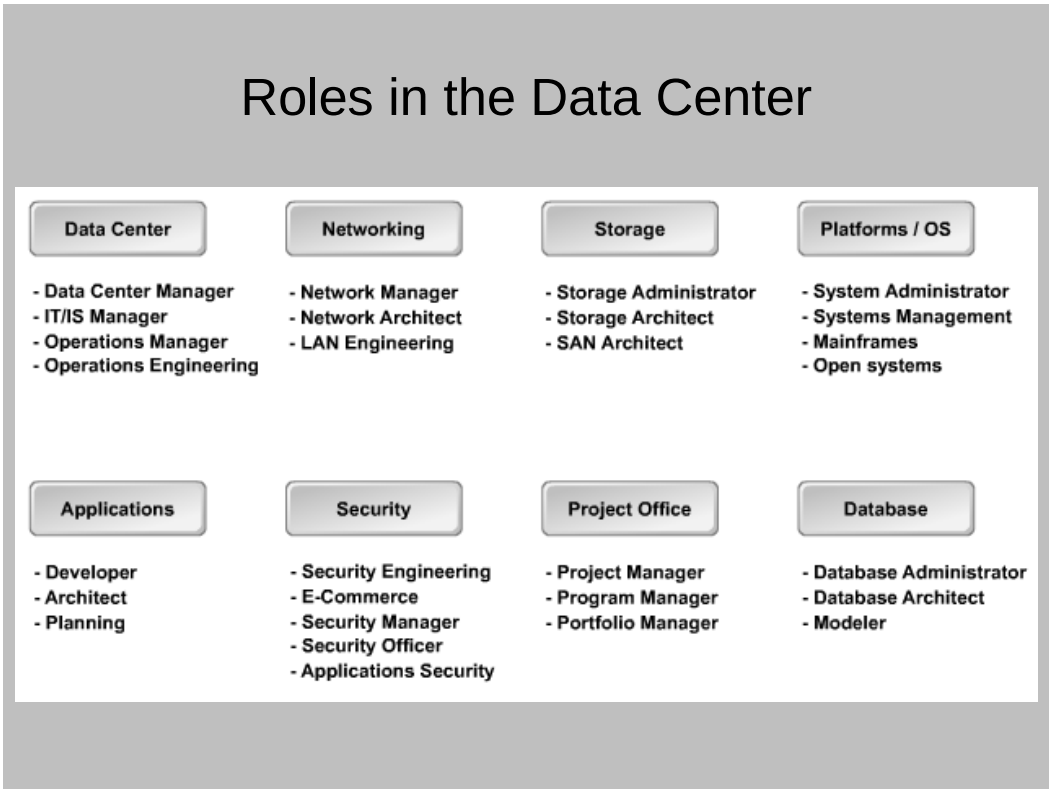
স্টোরেজ, প্ল্যাটফর্ম, ডাটাবেস এবং নেটওয়ার্ক এর মতো প্রতিটি তথ্য প্রযুক্তির মৌলিক কার্যক্রম সম্পাদন করার জন্য আলাদা আলাদা দল আছে। কৌশলগত কার্যক্রমের মধ্যে আছে, সরবরাহকারী নির্বাচন (Vendor Selection), স্থাপত্য উন্নয়ন, মান নিরুপন এবং নতুন প্রযুক্তি অনুসন্ধান করা। বিভিন্ন প্রকল্পের অংশ হিসাবে এগুলোর বিশেষ প্রযুক্তি বাস্তবায়নে নকশা, সংস্থাপন, অন্যান্য গোষ্ঠীগুলির সাথে সমন্বয়, এবং প্রকল্প পরিচালনা অন্তর্ভুক্ত থাকতে পারে। সবশেষে রয়েছে, চলমান বিভিন্ন প্রযুক্তির সহয়তা, যেমন সমস্যা সমাধান, উচ্চ স্তরের সহায়তা, হালনাগাদ করা এবং সরবরাহকারীদের ব্যবস্থাপনা করা। এই প্রকৌশলীগণ সাধারণত নেটওয়ার্ক নিয়ন্ত্রণ কেন্দ্র (Network Operation Center (NOC)) ও নিরাপত্তা নিয়ন্ত্রণ কেন্দ্র (Security Operation Center (SOC)) এর মাধ্যমে ডাটা সেন্টারের পরিষেবা প্রদান করেন। তাই জরুরী অবস্থায়, পরিষেবা অব্যাহত রাখতে তাদের পরিবহণের জন্য প্রয়োজনীয় গাড়ি ও গাড়ির চালক থাকা আবশ্যক।

প্রতিটি দল ক্রমাগত ব্যবসায়িক পুঁজি, পরিচালনা বাজেট এবং কর্মী সংখ্যা ব্যবহার করে সময়সীমা পূরণ, ব্যবসায়িক চাহিদা মেটানো এবং ব্যবসায়িক লক্ষ্য এবং সমস্যাগুলির সাথে প্রযুক্তি সমন্নয়করণের মতো কাজগুলো সম্পন্ন করে।



প্রধান আর্থিক কর্মকর্তা (CFO), প্রধান তথ্য কর্মকর্তা (CIO), প্রধান প্রযুক্তি কর্মকর্তা (CTO) এবং প্রধান তথ্য নিরাপত্তা কর্মকর্তা (CISO) -এর মতো কর্পোরেট ব্যবস্থাপক ডাটা সেন্টারের পরিচালনায় উল্লেখযোগ্য প্রভাব বিস্তার করে।

অনেক ডাটা সেন্টারে ব্যবস্থাপক হিসাবে নির্দিষ্ট নামযুক্ত পদ বিদ্যমান নাও থাকতে পারে, তবে কার্যক্রম অবশ্যই চলে। এই উদাহরণে ব্যক্তিদের বিচ্ছিন্ন ভূমিকার বদলে সম্মিলিত কার্যক্রমের রূপরেখা দেখানো হয়েছে। অনেক ক্ষেত্রে, এই ফাংশনগুলি ডাটা সেন্টারের বিভিন্ন ব্যক্তি এবং দলের ভূমিকার সম্মিলন ঘটায়।



১০. উপসংহার (Conclusion)

ডাটা সেন্টারের জন্য সাধারণভাবে স্বীকৃত তিনটি প্রধান ব্যবসায়িক প্রভাবক রয়েছে। তথ্য প্রযুক্তি পরিচালনার দক্ষতার সর্বোচ্চ ব্যবহার দ্বারা সম্প্রসারণের মাধ্যমে তথ্য চুরি বন্ধ করে ব্যবসাকে রক্ষা করে। পরিবর্তনশীল ব্যবসায়িক চাহিদার সাথে ডাটা সেন্টারকে খাপ খাওয়ানোর মাধ্যমে তথ্য প্রযুক্তি ব্যবস্থা সম্প্রসারণযোগ্য, নমনীয় এবং সহজ পদ্ধতিতে সম্প্রসারিত হবে।

আইন, প্রবিধান, এবং অন্যান্য সঙ্গতির (Compliance) প্রয়োজনীয়তা দ্রুত বাড়ছে। এর মধ্যে উল্লেখযোগ্য কয়েকটি প্রবিধান হলঃ Sarbanes-Oxley Act (SOX), যা আন্তর্জাতিকভাবে স্বীকৃত; এবং Basel II, যা আর্থিক প্রতিষ্ঠানে বিশ্বব্যাপী ব্যবহৃত হয়।

এসমস্ত বিষয় তথ্য ব্যবস্থাপনা কৌশলকে প্রভাবিত করে, কিন্তু প্রায়ই, একটি ডাটা সেন্টার থেকে ঠিক কি করা প্রয়োজন তা বুঝা কঠিন এবং সঠিকভাবে পরিমাপ করা আরো কঠিন হতে পারে। যাহোক, কিছু বিষয় আছে যা সব না হলেও অধিকাংশ নিয়মের অংশ। এর মধ্যে আছে চিঠিপত্র, চুক্তি ইত্যাদি নিরীক্ষা (Audit) করা, রেকর্ড দীর্ঘমেয়াদের জন্য সংরক্ষণ করা এবং প্রতিষ্ঠানের সমস্ত তথ্যের জন্য সংরক্ষণ ও মুছে ফেলার নীতির অনুমোদন দেওয়া।

তবে, প্রবিধান অবশ্যই প্রতিটি প্রতিষ্ঠানের বিশেষ পরিস্থিতি এবং বাংলাদেশের ক্ষেত্রে প্রযোজ্য তথ্য ব্যবস্থাপনার কৌশলের আলোকে ব্যাখ্যা ও অনুবাদ করতে হবে। প্রতিষ্ঠানের সঠিক চাহিদা নিরূপণ করতে হবে এবং তাদের নিজস্ব তথ্য ব্যবস্থাপনা কৌশলে এর প্রতিফলন থাকতে হবে।

উপরের বিষয়গুলি বিবেচনা করে এবং দ্রুত পরিবর্তনশীল প্রযুক্তি ও ব্যবসায়ের ভৌগলিক গুরুত্ব বিবেচনায় নিয়ে এই নির্দেশিকা একটি চলমান নথি হিসাবে বিবেচনা করা দরকার, যা নিয়মিত পর্যালোচনা ও হালনাগাদের দাবি রাখে।

List of Acronyms

Acronym	Full Name
TIA	Telecommunications Industry Association
SPOF	Single point of failure
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
LEED	Leadership in Energy and Environmental Design
HVAC	Heating, ventilation, and air conditioning
HVAC+R	heating, ventilation, air conditioning and refrigeration
BDS	Bangladesh Standard
IEC	International Electrotechnical Commission
ISMS	Information security management system
PCI	Payment card industry
DSS	Data Security Standard
COBIT	Control Objectives for Information and Related Technologies
ISACA	Information Systems Audit and Control Association
ICTDR	ICT Disaster Recovery
ITIL	Information Technology Infrastructure Library
SRG	Synergy Research Group
PDUs	Power distribution units
EMI	Electromagnetic Interference
UPS	Uninterruptible power supply
LT	Linear Technology
TPN Bus Bar	Task-positive network Bus Bar
RAF	Risk Assessment Framework
IP	Internet Protocol
LED	Light-emitting diode
LAN	Local area network
WAN	Wide-area network
VLAN	Virtual LAN
DR	Disaster Recovery
PVLAN	Private VLAN
SLA	Service-level agreement
IOPS	Input/output operations per second
DMZ	Demilitarized zone
IDS	Integrated Data Store
VPN	Virtual private network
SIEM	Security information and event management
WAF	web application framework

DLP	Data level parallelism
CTI	Cyber Threat Intelligence
CFO	Chief financial officer
CIO	Chief information officer
CTO	Chief technology officer
CISO	Chief information security officer
TVSS	Transient Voltage Surge Suppressor
MMSB	Multiple Message Switch Buffer
VPS	Virtual Private Server

১৩. শব্দকোষ (Glossary)

ক্রম	শব্দ/ বিষয়	সংজ্ঞা
১	তারের অবকাঠামো (Cabling Infrastructure)	টেলিকমিউনিকেশনে স্ট্রাকচার্ড ক্যাবলিং হ'ল ক্যাবলিং ইনফ্রাস্ট্রাকচার যা অনেকগুলি স্ট্যান্ডার্ডাইজড ছোট উপাদান (যার ফলে কাঠামোগত)বা সাবসিস্টেমগুলি নিয়ে গঠিত।
২	তারকা টোপোলজি (Star Topology)	যে টপোলজি একটি কেন্দ্রীয় নিয়ন্ত্রণকারী কম্পিউটার বা হস্ত কম্পিউটারের সাথে অন্যান্য কম্পিউটার সংযুক্ত করে নেটওয়ার্ক গরে তোলে তাকে স্টার টপোলজি বলা হয়। এক্ষেত্রে একটি কম্পিউটার কেন্দ্রীয় কম্পিউটারের মাধ্যমে তথ্য আদান প্রদান করে থাকে।
৩	বাড়তি (reduntant)	প্রয়োজনের অতিরিক্ত সার্ভার, স্টোরেজ বা নেটওয়ার্ক উপাদান যা কোন কারণের মূল উপাদানের অপ্রাপ্যতার সময় প্রয়োজনীয় পরিষেবা প্রদান করতে পারে।
৪	ব্যর্থতার একক বিন্দু (Single Point of Failure)	ব্যর্থতার একক পয়েন্ট)SPoFএকটি (সিস্টেমের এমন একটি অংশ যা যদি এটি ব্যর্থ হয় তবে পুরো সিস্টেমটি কাজ করা বন্ধ করে দেবে। উচ্চ প্রাপ্যতা বা নির্ভরযোগ্যতা সম্পন্ন সিস্টেমে SPoF অনাকাঙ্ক্ষিত।
৫	প্রাপ্যতা	অপারেশনের সময় একটি সিস্টেম, সাবসিস্টেম বা সরঞ্জাম চালু থাকার সম্ভব্যতা।
৬	তাপ, বায়ু চলাচল, শীতাতপ নিয়ন্ত্রণ (HVAC)	তাপ, বায়ু চলাচল, শীতাতপ নিয়ন্ত্রণ (HVAC) হ'ল স্থাপনা ও যানবাহনের আভ্যন্তরীন পরিবেশগত স্বাচ্ছন্দ্য প্রদানের প্রযুক্তি। এর লক্ষ্য হ'ল আরামদায়ক তাপমাত্রা এবং গ্রহণযোগ্য বায়ু প্রবাহ নিশ্চিত করা।
৭	তথ্য নিরাপত্তা ব্যবস্থাপনা প্রক্রিয়া (ISMS)	তথ্য নিরাপত্তা ব্যবস্থাপনা (ISMS) হ'ল হুমকি এবং দুর্বলতা থেকে সম্পদের গোপনীয়তা, সহজলভ্যতা এবং অখণ্ডতা সুরক্ষা নিশ্চিত করার জন্য কোনও সংস্থাকে যেসব নীতি বাস্তবায়ন করা দরকার এমন নিয়ন্ত্রণগুলি বর্ণনা করে।
৮	PCI-DSS	পেমেন্ট কার্ড ইন্ডাস্ট্রি ডেটা সিকিউরিটি স্ট্যান্ডার্ড)PCI-DSSএমন সংস্থাগুলির জন্য (একটি তথ্য সুরক্ষা মান যারা স্বীকৃত ক্রেডিট কার্ড স্কিম পরিচালনা করে।
৯	ক্লাউড কম্পিউটিং	ক্লাউড কম্পিউটিং)Cloud Computing) হচ্ছে কম্পিউটার রিসোর্স যেমন - কম্পিউটার হার্ডওয়্যার ওসফটওয়্যার, নেটওয়ার্ক ডিভাইস প্রভৃতি ব্যবহার করে কম্পিউটার নেটওয়ার্কের মাধ্যমে কোনো সার্ভিস বা সেবা প্রদান করা। ক্লাউড (বিশেষত ইন্টারনেট) কম্পিউটিং কোনো নির্দিষ্ট টেকনোলজি নয়, বেশ কয়েকটি টেকনোলজিকে কাজে লাগিয়ে তৈরি করা একটা ব্যবসায়িক মডেল বা বিশেষ পরিসেবা।
১০	সার্ভার	একটি সার্ভার হল ভোক্তা থেকে অনুরোধ গ্রহণ এবং সে অনুযায়ী তার প্রতিউত্তরে সক্ষম সফটওয়্যার। সার্ভার যে কোন কম্পিউটারে চলতে পারে, নিয়োজিত করা কম্পিউটারকে একক ভাবে বুঝায়। "সার্ভার"
১১	দুর্যোগ পরবর্তী তথ্য	আইসিটি দুর্যোগ পুনরুদ্ধার হল একটি বড় ধরনের ব্যাঘাতের পরে সিস্টেমগুলি পুনরুদ্ধারের

	পুনরুদ্ধার (ICT DR)	প্রক্রিয়া।
১২	ইন্টারনেটযুক্ত সামগ্রী (IoT)	ইন্টারনেট অব থিংস কে সংক্ষেপে আইওটি বলে, যার বাংলা অর্থ হল বিভিন্ন জিনিসপত্রের সাথে ইন্টারনেটের সংযোগ।
১৩	অভিযোজনযোগ্য (Adaptable)	নতুন অবস্থার সাথে সামঞ্জস্য করতে সক্ষম।
১৪	অবিচ্ছিন্ন শক্তি সরবরাহ (ইউপিএস)	ইউপিএস)UPS) এমন একটি ইলেক্ট্রিক্যাল ডিভাইস)Electrical Device) যা কিছু সময়ের জন্য বিদ্যুৎ সঞ্চয় করে রাখতে পারে এবং যেকোন মুহূর্তে কম্পিউটার ও অন্যান্য যন্ত্রপাতিতে বিদ্যুৎ সরবরাহ করতে পারে।
১৫	র‍্যাকের সারি (Rack aisle)	ডাটা সেন্টারে সার্ভারগুলো সাধারণত একাধিক র‍্যাকে সাজিয়ে রাখা হয়। এই র‍্যাকগুলি পাশাপাশি সন্নিবিষিত হয়। এটিই হল র‍্যাকের সারি।
১৬	র‍্যাকের বিন্যাস (Rack Configuration)	র‍্যাকগুলো সাধারণত একক বা দ্বৈত সারি বিন্যাসে রাখা হয়।
১৭	উত্তপ্ত এলাকা (Hot Spot)	চারপাশের তুলনায় তুলনামূলকভাবে গরম তাপমাত্রা একটি ছোট।
১৮	শীতাতপ নিয়ন্ত্রণ (Air Condition)	শীতাতপ নিয়ন্ত্রণ ব্যবস্থা হচ্ছে অভ্যন্তরীন বাতাসে)indoor air) আর্দ্রতার পরিমাণ নিয়ন্ত্রণ করে আরামদায়ক পরিবেশ তৈরী। বিশদ অর্থে শীতলীকরন, তাপমাত্রা বৃদ্ধি, বাতাসের গতি নিয়ন্ত্রণ ও বিশুদ্ধতা নিশ্চিতকরণই শীতাতপ নিয়ন্ত্রণ ব্যবস্থা।
১৯	র‍্যাক (Rack)	ডাটা সেন্টারে সার্ভার রাখার জন্য আলমিরা সদৃস কাঠামো।
২০	স্তর (Tier)	তথ্যের প্রাপ্যতার উপর নির্ভর করে আরোপিত ডাটা সেন্টারের সংখ্যা মান
২১	উচ্চ-প্রাপ্যতা (High Availability)	উচ্চ প্রাপ্যতা একটি সিস্টেমের বৈশিষ্ট্য, যার লক্ষ্য সাধারণ সময়ের চেয়ে উচ্চতর সময়ের জন্য অপারেশনাল পারফরম্যান্সের প্রাপ্যতা নিশ্চিত করা।
২২	স্থাপত্য (Architecture)	স্থাপত্য হ'ল একটি কম্পিউটার নেটওয়ার্কের নকশা। এটি একটি নেটওয়ার্কের বাহ্যিক উপাদান এবং তাদের কার্যকরী সংগঠন এবং কনফিগারেশন, এর অপারেশনাল নীতি এবং পদ্ধতি এবং সেই সাথে ব্যবহৃত যোগাযোগ প্রোটোকলগুলির নির্দিষ্টকরণের জন্য একটি কাঠামো।
২৩	কার্যকরী মেঝে ফলক	ডাটা সেন্টারে ব্যবহৃত বিশেষায়িত টাইলস।
২৪	বজ্র নিরোধক দন্ড (Lightening	এটি একটি ধাতব রড যা বজ্রপাতের হাত থেকে রক্ষা করার উদ্দেশ্যে কোনও ভবনের উপরে বসানো হয়। যদি বজ্রপাত ভবনকে আঘাত করে, তবে এটি বজ্র নিরোধক দন্ডকে আঘাত করবে এবং তারের মধ্য দিয়ে সঞ্চালিত হবে, নতুবা বজ্রপাত থেকে আগুনের সূত্রপাত করতে

	Rod)	পারে বা ভবনটি বিদ্যুতায়িত হতে পারে।
২৫	ঢাকনা (Screening)	ছাদে স্থাপিত যন্ত্রাংশকে বাহ্যিক ক্ষতি হতে রক্ষা করতে ব্যবহৃত আচ্ছাদন।
২৬	বিদ্যুৎ বিতরণ ব্যবস্থা (PDU)	একটি বিদ্যুৎ বিতরণ ব্যবস্থা (PDU) এমন একটি ডিভাইস যাতে ডাটা সেন্টারের মধ্যে থাকা নেটওয়ার্কিং সরঞ্জাম ও র‍্যাকগুলিতে বৈদ্যুতিক শক্তি বিতরণ করার জন্য একাধিক আউটপুটগুলিতে লাগানো।
২৭	উত্থিত মেঝের ব্যবস্থা (Raised floor systems)	একটি উত্থিত মেঝে যান্ত্রিক এবং বৈদ্যুতিক পরিষেবাগুলির বিতরণের জন্য একটি লুকানো শূন্যতা তৈরি করার জন্য বাহ্যিক মেঝের উপরে একটি উচ্চতর কাঠামোগত মেঝে সরবরাহ করে।
২৮	ছিদ্রযুক্ত উত্থিত মেঝে (Perforated Raised Floor)	ছিদ্রযুক্ত উত্থিত মেঝে ডাটা সেন্টারে নির্বিঘ্ন বায়ু চলাচল নিশ্চিত করে।
২৯	প্যাচ ফলক (patch panels)	একটি প্যাচ প্যানেল এমন একটি ডিভাইস বা ইউনিট যা সাধারণত একই বা অনুরূপ প্রকারের বেশ কয়েকটি জ্যাক সমন্বিত করে যাতে সুবিধাজনক, নমনীয় উপায়ে সার্কিটগুলি পর্যবেক্ষণ, আন্তঃসংযোগ স্থাপন এবং পরীক্ষার জন্য সংযোগ ও রাউটিং সার্কিট ব্যবহার করতে হয়। প্যাচ প্যানেলগুলি সাধারণত কম্পিউটার নেটওয়ার্কিং, রেকর্ডিং স্টুডিও, রেডিও এবং টেলিভিশনে ব্যবহৃত হয়।
৩০	বৈদ্যুতিক তারের আবরক নল (conduits)	বৈদ্যুতিক তারের আবরক নল যা কোনও বিল্ডিং বা কাঠামোতে বৈদ্যুতিক ওয়্যারিং সুরক্ষিত ও রুট করার জন্য ব্যবহৃত হয়।
৩১	জরুরী সংযোগ বিচ্ছিন্নকরন (Shutdown)	কোন ধরণের নিরাপত্তা ঝুঁকি সৃষ্টি হলে বাইরের সাথে ডাটা সেন্টারের নেটওয়ার্ক সংযোগ বিচ্ছিন্নকরণ।
৩২	গ্রাউন্ডিং এবং বন্ডিংয়ের (grounding and bonding)	বিদ্যুৎ বর্তনীর ভুমির সাথে সংযোগ।
৩৩	মেস (Mesh)	যদি কোনো নেটওয়ার্কে ডিভাইস বা কম্পিউটারগুলোর মধ্যে অতিরিক্ত সংযোগ থাকে তাহলে তাকে বলা হয় মেশ টপোলজি।
৩৪	উচ্চ কম্পাংকের প্রতিবন্ধকতা (high-frequency impedance)	প্রতিবন্ধকতা বলতে কোনও পরিবর্তী বৈদ্যুতিক বর্তনীর মধ্যে দিয়ে পরিবর্তী বিদ্যুৎপ্রবাহ প্রবাহিত হবার সময় বর্তনীটি যে মোট বাধা সৃষ্টি করে, তাকে বোঝায়।

৩৫	প্রাসঙ্গিক সাংকেতিক গরাদ (SRG)	উচ্চ কম্পাংকের প্রতিবন্ধকতা এড়াতে ব্যবহৃত প্রতিরক্ষা ফলক।
৩৬	বর্তনী বিচ্ছিন্নকারক (circuit breakers)	একটি সার্কিট ব্রেকার একটি স্বয়ংক্রিয়ভাবে চালিত বৈদ্যুতিক সুইচ যা কোনও ওভারলোড বা শর্ট সার্কিট থেকে অতিরিক্ত বিদ্যুৎ প্রবাহের কারণে বৈদ্যুতিক সার্কিটকে রক্ষা করার জন্য ডিজাইন করা হয়। এর মূল কাজটি একটি ত্রুটি সনাক্ত করার পরে বিদ্যুৎ প্রবাহকে বাধা দেওয়া।
৩৭	স্থির বৈদ্যুতিক স্রবন (electrostatic discharge)	স্থির বৈদ্যুতিক স্রবন হ'ল সংস্পর্শের ফলে বৈদ্যুতিক চার্জযুক্ত দুটি বস্তুর মধ্যে বৈদ্যুতিক সংক্ষিপ্ত প্রবাহ।
৩৮	তড়িৎ চৌম্বকীয় হস্তক্ষেপ (EMI)	তড়িৎ চৌম্বকীয় হস্তক্ষেপ (ইএমআই), যাকে রেডিও ফ্রিকোয়েন্সি হস্তক্ষেপ বলা (আরএফআই) হয় যখন রেডিও ফ্রিকোয়েন্সি স্পেকট্রামে হয় একটি বাহ্যিক উৎস দ্বারা উৎপাদিত ঝামেলা যা বৈদ্যুতিক চৌম্বকীয় আনয়ন, তড়িৎক্ষেত্রের সংযোগ বা বাহন দ্বারা বৈদ্যুতিক সার্কিটকে প্রভাবিত করে।
৩৯	বিদ্যুৎ শর্তকরণ (power-conditioning) সরঞ্জাম	বিদ্যুতের আশানুরূপ প্রবাহ নিশ্চিতকারী যন্ত্র
৪০	LT প্যানেল	এলটি প্যানেল একটি বৈদ্যুতিক বিতরণ বোর্ড যা জেনারেটর বা ট্রান্সফর্মার থেকে বিদ্যুৎ গ্রহণ করে এবং বিভিন্ন বৈদ্যতিক যন্ত্র এবং বিতরণ বোর্ডগুলিতে বিদ্যুৎ বিতরণ করে
৪১	TPN Bus Bar	বৈদ্যুতিক শক্তি বিতরণে, একটি বাসবার একটি ধাতব স্ট্রিপ বা বার হয় যা সাধারণত স্থানীয় উচ্চ বিদ্যুত বিতরণের জন্য সুইচ, প্যানেল বোর্ড এবং বাসওয়ের ঘেরের অভ্যন্তরে থাকে।
৪২	MMSB	এটি একধরণের স্যুইচ বোর্ড।
৪৩	তথ্য সংরক্ষণাগার (Storage)	তথ্য জমা রাখার জন্য বিশেষায়িত সার্ভার।
৪৪	Signal Reference Ground (SRG)	সার্ভার ও এর র‍্যাককে গ্রাউন্ডিং করার প্রযুক্তি
৪৫	শীতলীকারক নিমজ্জিত তরল (Immersion Cooling Fluid)	তরল প্রবাহের মাধ্যমে শীতলীকরণ।
৪৬	পানি ছিটানোর যন্ত্র	একটি পানি ছিটানোর যন্ত্র একটি অগ্নি প্রতিরোধক ব্যবস্থার উপাদান যা পূর্বনির্ধারিত

	(sprinkler)	তাপমাত্রা ছাড়িয়ে যাওয়ার পরে পানি ছড়িয়ে দেয়।
৪৭	সার্ভারের দেরাজ (Cabinet)	সার্ভার র‍্যাকের অন্য নাম।
৪৮	আইপি (IP)	ইন্টারনেট প্রোটোকল নেটওয়ার্কের সীমানা জুড়ে ডেটাগ্রাম রিলে করার জন্য (আইপি) ইন্টারনেট প্রোটোকল স্যুটে মূলযোগাযোগ প্রোটোকল।
৪৯	অবলোহিত (Infrared) রশ্মি	যে সকল তড়িৎ চৌম্বক বিকিরণের তরঙ্গ দৈর্ঘ্যের সীমা ১ মাইক্রোমিটার থেকে ১ মিলিমিটার পর্যন্ত বিস্তৃত তাদের বলা হয় অবলোহিত রশ্মি।
৫০	LED	এলইডি এমন একটি অর্ধপরিবাহী যন্ত্রাংশ যা আলো বিকিরণ করে।
৫১	লাক্স (LUX)	লাক্স হ'ল আলোকের এসআই উদ্ভূত ইউনিট, প্রতি ইউনিট ক্ষেত্রের মধ্যে আলোকিত ফ্লাক্স পরিমাপ করে।
৫২	জংশন বাক্স	বিভিন্ন তারের মধ্যে সংযোগের জন্য যে বাক্স ব্যবহার করা হয়।
৫৩	ওহম (Ohm)	ওহম বা ও'ম হল রোধের SI বা আন্তর্জাতিক পদ্ধতির একক।
৫৪	কক্ষের মাঝে কক্ষ (Room in Room)	এক কক্ষের মাঝে আরেক কক্ষ। সাধারনত, ডেটা সেন্টারে গুরুত্বপূর্ণ ডিভাইসগুলো আলাদা কক্ষে রেখে সেগুলো অন্তরীন করে রাখা হয়। অনেক সময় একে Enclosure ও বলা হয়।
৫৫	ভয়েস ওভার আইপি (VoIP)	ভিওআইপি (VoIP) এর পূর্ণরূপ হলো Voice Over Internet Protocol. এটি ইন্টারনেটের মাধ্যমে কথা বলার এক ধরনের মাধ্যম। মোবাইল দিয়ে বিশ্বের এক দেশ থেকে অন্য দেশে কথ বলা এমনকি একই দেশের মধ্যে এক স্থান থেকে অন্য স্থানে কথা বলার ক্ষেত্রে ভিওআইপি ব্যবহৃত হয়। আর এজন্য অবশ্যই ইন্টারনেট থাকতে হবে। এ পদ্ধতিতে দেশ থেকে বিদেশে কথা বললে অরিজিনেশন এবং বিদেশ থেকে কথা বললে টারমিনেশন হয়।
৫৬	QoS	পরিষেবার গুণমান (QoS) এমন কোনও প্রযুক্তিকে বোঝায় যা নেটওয়ার্কে প্যাকেট ক্ষয়, বিলম্ব এবং ঝাঁকুনি হ্রাস করতে ডেটা ট্র্যাফিক পরিচালনা করে। QoS নেটওয়ার্কে নির্দিষ্ট ধরণের ডেটার জন্য অগ্রাধিকার নির্ধারণ করে নেটওয়ার্ক সংস্থান নিয়ন্ত্রণ করে এবং পরিচালনা করে।
৫৭	LAN	লোকাল এরিয়া নেটওয়ার্ক (ল্যান) (Local Area Network বা LAN) অর্থাৎ স্থানীয় অঞ্চলের নেটওয়ার্ক হলো একটি কম্পিউটার নেটওয়ার্ক যা বাড়ি, বিদ্যালয়ে, কম্পিউটার ল্যাবরেটরি বা অফিসের একটি সীমিত এলাকার একাধিক কম্পিউটারের মধ্যে আন্তঃসংযোগস্থাপন করে থাকে।
৫৮	WAN	একটি প্রশস্ত অঞ্চল নেটওয়ার্ক (WAN) একটি টেলিযোগাযোগ নেটওয়ার্ক যা কম্পিউটার নেটওয়ার্কিংয়ের প্রাথমিক উদ্দেশ্যে একটি বিশাল ভৌগলিক অঞ্চল জুড়ে বিস্তৃত। ওয়াইড এরিয়া নেটওয়ার্কগুলি প্রায়শই লিজড টেলিযোগযোগ সার্কিটের সাথে প্রতিষ্ঠিত হয়।

৫৯	ভিডিও স্ট্রিমিং (Video Streaming)	ভিডিও স্ট্রিমিং হ'ল মাল্টিমিডিয়া যা নিয়মিত সরবরাহকারীর মাধ্যমে সরবরাহ করার সময় শেষ ব্যবহারকারীকে দ্বারা গ্রহণ করা হয় এবং উপস্থাপিত হয়। "টু স্ট্রিম" ক্রিয়াটি এই পদ্ধতিতে মিডিয়া সরবরাহ করা বা প্রাপ্তির প্রক্রিয়া বোঝায়।
৬০	VLAN	ভার্চুয়াল ল্যান (Virtual LAN) হ'ল এমন কোনও সম্প্রচার ডোমেন যা ডেটা লিঙ্ক স্তর (Data Link, OSI স্তর 2) এ কম্পিউটার নেটওয়ার্কে বিভাজনিত এবং বিচ্ছিন্ন থাকে। ল্যান স্থানীয় অঞ্চল নেটওয়ার্কের সংক্ষিপ্ত রূপ এবং এই প্রসঙ্গে ভার্চুয়াল একটি শারীরিক বস্তুকে পুনরায় তৈরি করা এবং অতিরিক্ত যুক্তি দ্বারা পরিবর্তিত করে। ভিএলএএনরা নেটওয়ার্ক ফ্রেমে ট্যাগ প্রয়োগ করে এবং নেটওয়ার্কিং সিস্টেমে এই ট্যাগগুলি হ্যান্ডল করে কাজ করে - একটি নেটওয়ার্কে শারীরিকভাবে থাকা নেটওয়ার্ক ট্র্যাফিকের উপস্থিতি এবং কার্যকারিতা তৈরি করে তবে এটি পৃথক নেটওয়ার্কের মধ্যে বিভক্ত হয়ে কাজ করে।
৬১	DR	দুর্যোগ পুনরুদ্ধার (DR) সুরক্ষা পরিকল্পনার একটি ক্ষেত্র যা লক্ষ্য করে যে কোনও সংস্থাকে উল্লেখযোগ্য নেতিবাচক ইভেন্টগুলির প্রভাব থেকে রক্ষা করা। জায়গায় একটি দুর্যোগ পুনরুদ্ধার কৌশল হ'ল একটি সংস্থাকে একটি বাধাগ্রস্থ হওয়ার পরে জরুরী গুরুত্বপূর্ণ কার্যকলাপ বজায় রাখতে বা দ্রুত পুনরায় শুরু করতে সক্ষম করে।
৬২	তথ্য প্রতিলিপি (Replication)	সফ্টওয়্যার বা হার্ডওয়্যার উপাদানগুলির মতো নির্ভরযোগ্যতা, ত্রুটি-সহনশীলতা বা অ্যাক্সেসযোগ্যতার উন্নতি করার জন্য অপ্রয়োজনীয় সংস্থানগুলির মধ্যে যেমন অনর্থক সংস্থানগুলির মধ্যে ধারাবাহিকতা নিশ্চিত করার জন্য কম্পিউটিংয়ের প্রতিরূপ জড়িত।
৬৩	কাঠামোগত ক্যাবলিং সিস্টেম (SCS)	একটি স্ট্রাকচার্ড ক্যাবলিং সিস্টেমটি ক্যাবলিং এবং সম্পর্কিত হার্ডওয়্যারগুলির একটি সম্পূর্ণ সিস্টেম, যা একটি বিস্তৃত টেলিযোগাযোগ অবকাঠামো সরবরাহ করে। এই অবকাঠামোটি বিস্তৃত ব্যবহারগুলিতে পরিবেশন করে, যেমন টেলিফোন পরিষেবা সরবরাহ করা বা কম্পিউটার নেটওয়ার্কের মাধ্যমে ডেটা প্রেরণ করা। এটি ডিভাইস নির্ভর না হওয়া উচিত।
৬৪	পরিষেবা স্তরে চুক্তি (SLA)	একটি পরিষেবা-স্তরের চুক্তি (SLA) কোনও পরিষেবা সরবরাহকারী এবং তার গ্রাহকদের মধ্যে একটি চুক্তি যা সরবরাহকারীর পরিষেবাগুলি কী সরবরাহ করবে এবং সেই পরিষেবা মান নির্ধারণ করবে যা সরবরাহকারী মেনে চলতে বাধ্য থাকে।
৬৫	সার্ভার ভার্চুয়ালাইজেশন (VPS)	এটি একটি ভার্চুয়াল হোস্টিং মেশিন, যা একটি ইন্টারনেট হোস্টিং পরিষেবা দ্বারা পরিষেবা হিসাবে বিক্রি হয়।
৬৬	স্টোরেজ এরিয়া নেটওয়ার্ক (SAN)	স্টোরেজ এরিয়া নেটওয়ার্ক (SAN) হ'ল একটি ডেডিকেটেড হাই স্পিড নেটওয়ার্ক বা সাবনেটওয়ার্ক যা একাধিক সার্ভারে স্টোরেজ ডিভাইসের ভাগ করা পুলকে আন্তঃসংযোগ করে এবং উপস্থাপন করে। একটি SAN সাধারণ ব্যবহারকারীর নেটওয়ার্ক থেকে স্টোরেজ রিসোর্সগুলি সরিয়ে নিয়ে যায় এবং তাদের একটি স্বাধীন, উচ্চ-কর্মক্ষমতা নেটওয়ার্কে পুনর্গঠিত করে।
৬৭	টেপ লাইব্রেরি (Tape Library)	টেপ লাইব্রেরি হ'ল একটি উচ্চ-ক্ষমতা সম্পন্ন স্টোরেজ সিস্টেম যা টেপ কার্তুজগুলি সংরক্ষণ, পুনরুদ্ধার, পড়ার এবং লেখার জন্য ব্যবহৃত হয়। একটি টেপ লাইব্রেরিতে টেপ কার্টরিজগুলি স্বয়ংক্রিয়ভাবে পরিবর্তনের জন্য ব্যবহৃত রোবোটিক সিস্টেম সহ কার্তুজগুলি এবং একাধিক

টেপ ড্রাইভ রয়েছে।

৭০	বাহ্যিক কাঠামো (Chassis)	চ্যাসিস হ'ল একটি কৃত্রিম বস্তুর লোড-ভারবহন কাঠামো, যা কাঠামোগতভাবে তার নির্মাণ এবং কার্যকরীভাবে অবজেক্টটিকে সমর্থন করে। চ্যাসিসের উদাহরণ একটি গাড়ির ফ্রেম, মোটর গাড়ির আন্ডার পার্ট, যার উপরে দেহটি মাউন্ট করা হয়; যদি চলমান গিয়ার যেমন চাকা এবং সংক্রমণ, এবং কখনও কখনও এমনকি ড্রাইভারের আসনও অন্তর্ভুক্ত থাকে।
৭১	নিগূঢ় প্রতিরক্ষা (Defense-in-Depth)	Defense-in-Depth সাইবারসিকিউরিটির একটি দৃষ্টিভঙ্গি, যাতে মূল্যবান তথ্য এবং তথ্য সুরক্ষার জন্য একাধিক প্রতিরক্ষামূলক ব্যবস্থা স্তরযুক্ত হয়। যদি একটি মেকানিজম ব্যর্থ হয়, অন্য আক্রমণ তাৎক্ষনিক পদক্ষেপ নেয়।
৭২	তথ্য নিরাপত্তা প্রশাসক (Information Security Administrator)	তথ্য প্রযুক্তির নিরাপত্তা বা সুরক্ষা প্রশাসক কোনও সংস্থার মধ্যে সমস্ত আইটি-সংক্রান্ত সুরক্ষা এবং সুরক্ষা সম্পর্কিত সমস্যাগুলি পরিচালনা করার জন্য দায়বদ্ধ। এর মধ্যে বিকাশকারী সিস্টেম এবং নীতি অন্তর্ভুক্ত থাকতে পারে, পাশাপাশি সংস্থা এবং গ্রাহক উভয় ডেটা সুরক্ষিত করার জন্য প্রক্রিয়াগুলির বাস্তবায়ন তদারকি করতে পারে
৭৩	অননুমোদিত অভিগমন (Unauthorized Access)	অননুমোদিত অ্যাক্সেস হ'ল যখন কেউ কোনও ওয়েবসাইট, প্রোগ্রাম, সার্ভার, পরিষেবা বা অন্য কারও অ্যাকাউন্ট বা অন্যান্য পদ্ধতি ব্যবহার করে অন্য সিস্টেমে অ্যাক্সেস পান। উদাহরণস্বরূপ, যদি কেউ এমন কোনও অ্যাকাউন্টের জন্য পাসওয়ার্ড বা ব্যবহারকারীর নাম অনুমান করতে থাকে যা অ্যাক্সেস না পাওয়া পর্যন্ত তাদের নয়, তবে এটিকে অননুমোদিত অ্যাক্সেস হিসাবে বিবেচনা করা হবে।
৭৪	অসামরিকীকৃত এলাকা (Demilitarized Zone (DMZ))	ডিএমজেড, ডিমিলিটারাইজড জোনটির (Demilitarized Zone) জন্য সংক্ষিপ্ত, একটি নেটওয়ার্ক (বাহ্যিক বা যৌক্তিক, Physical or Logical) হোস্টগুলি সংযোগ করতে ব্যবহৃত হয় যা একটি অবিশ্বস্ত বাহ্যিক নেটওয়ার্ক - সাধারণত ইন্টারনেট - অভ্যন্তরীণ, প্রাইভেট নেটওয়ার্ক রাখার সময় - সাধারণত কর্পোরেট নেটওয়ার্ক - আলাদা এবং বিচ্ছিন্ন হয়ে থাকে বাহ্যিক নেটওয়ার্ক গঠন।
৭৫	অনধিকার প্রবেশ প্রতিরোধ ব্যবস্থা (Intrusion Prevention System (IPS))	একটি অনধিকার অনুপ্রবেশ প্রতিরোধ ব্যবস্থা (IPS) এমন একধরনের নেটওয়ার্ক সুরক্ষা যা সনাক্তকারী হুমকিগুলি সনাক্ত ও প্রতিরোধ করতে কাজ করে। অনুপ্রবেশ প্রতিরোধ ব্যবস্থা সম্ভাব্য দূষিত ঘটনার সন্ধান এবং তাদের সম্পর্কে তথ্য ক্যাপচার করার জন্য আপনার নেটওয়ার্ককে অবিচ্ছিন্নভাবে পর্যবেক্ষণ করে।
৭৬	ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN)	ভার্চুয়াল প্রাইভেট নেটওয়ার্ক (VPN) এমন একটি নেটওয়ার্ক যা পাবলিক তারের ব্যবহার করে তৈরি করা হয় - সাধারণত ইন্টারনেট - কোনও সংস্থার ব্যক্তিগত, অভ্যন্তরীণ নেটওয়ার্কের সাথে প্রত্যন্ত ব্যবহারকারী বা আঞ্চলিক অফিসগুলিকে সংযুক্ত করতে।
৭৭	SIEM	কম্পিউটার সুরক্ষা, সুরক্ষা তথ্য এবং ইভেন্ট ম্যানেজমেন্ট (SIEM), সফ্টওয়্যার পণ্য ও পরিষেবাতে সিকিউরিটি ইনফরমেশন ম্যানেজমেন্ট (SIM) এবং সিকিউরিটি ইভেন্ট ম্যানেজমেন্ট (SEM) মিলিত হয়। তারা অ্যাপ্লিকেশন এবং নেটওয়ার্ক হার্ডওয়্যার দ্বারা

		উৎপাদিত সুরক্ষা সতর্কতাগুলির রিয়েল-টাইম বিশ্লেষণ সরবরাহ করে।
৭৮	ওয়েব এপ্লিকেশন ফায়ারওয়াল (WAF)	একটি ওয়েব অ্যাপ্লিকেশন ফায়ারওয়াল (WAF) হ'ল ফায়ারওয়াল যা কোনও ওয়েবসাইট বা ওয়েব অ্যাপ্লিকেশন থেকে এবং যাতায়াত করার সময় ডেটা প্যাকেটগুলি পর্যবেক্ষণ করে, ফিল্টার করে এবং ব্লক করে ওয়েব এপ্লিকেশন ফায়ারওয়াল। একটি WAF হয় নেটওয়ার্ক-ভিত্তিক, হোস্ট-ভিত্তিক বা ক্লাউড-ভিত্তিক এবং প্রায়শই একটি বিপরীত প্রক্সি মাধ্যমে স্থাপন করা হয় এবং এক বা একাধিক ওয়েবসাইট বা অ্যাপ্লিকেশনগুলির সামনে রাখা হয়।
৭৯	এন্টি-ডিডিওস (Anti-DDoS)	অ্যান্টি-ডিডিওস (পরিষেবার বিতরণ অস্বীকৃতি) অ্যান্টি-ডিডিওস সোর্স-ঠিকানায় ম্যালিসিয়াস বা দুষিত (Malicious) ট্র্যাফিক সনাক্ত করতে আচরণগত বিশ্লেষণ, ট্রাফিক স্বাক্ষর, হার সীমাবদ্ধকরণ এবং এই জাতীয় অন্যান্য কৌশল ব্যবহার করে। একবার আমরা দূষিত ট্র্যাফিকের উৎস চিহ্নিত করার পরে আমরা এটি কালো তালিকাভুক্ত করি।
৮০	ডেটা লস প্রোটেকশন (DLP)	ডেটা ক্ষতি প্রতিরোধের সফটওয়্যার সম্ভাব্য ডেটা লঙ্ঘন/ক্ষতি/সংক্রমণ সনাক্ত করে এবং ব্যবহারের সময়, গতিতে এবং বিশ্রামের সময়ে সংবেদনশীল ডেটা পর্যবেক্ষণ, সনাক্তকরণ এবং ব্লক করে তাদের বাধা দেয়। "ডেটা হ্রাস" এবং "ডেটা লিক" শব্দগুলি সম্পর্কিত এবং প্রায়শই পরিবর্তিতভাবে ব্যবহৃত হয়।
৮১	ডিএনএস (DNS)	ডোমেন নেম সিস্টেম (DNS) একটি নামকরণ ডাটাবেস যেখানে ইন্টারনেট ডোমেন নামগুলি অবস্থিত এবং ইন্টারনেট প্রোটোকল (IP) ঠিকানাগুলিতে অনুবাদ করা হয়। ডোমেন নেম সিস্টেমটি কোনও ওয়েবসাইট ওয়েবসাইট সনাক্ত করতে কম্পিউটার ব্যবহার করে এমন আইপি ঠিকানায় একটি ওয়েবসাইট সনাক্ত করতে লোকেরা যে নাম ব্যবহার করে তা ম্যাপ করে।
৮২	সাইবার থ্রেট ইন্টেলিজেন্স (CTI)	সাইবার হুমকি বুদ্ধিমত্তা হ'ল হুমকি এবং হুমকি আক্টরদের (Actor) তথ্য যা সাইবার স্পেসে ক্ষতিকারক ঘটনাগুলি প্রশমিত করতে সহায়তা করে। সাইবার হুমকি গোয়েন্দা সূত্রে ওপেন সোর্স ইন্টেলিজেন্স Open Source Intelligence, সোশ্যাল মিডিয়া ইন্টেলিজেন্স, হিউম্যান ইন্টেলিজেন্স, টেকনিক্যাল ইন্টেলিজেন্স বা গভীর এবং অন্ধকার-ওয়েব থেকে বুদ্ধিমত্তা অন্তর্ভুক্ত রয়েছে।
৮৩	নেটওয়ার্ক নিয়ন্ত্রণ কেন্দ্র (Network Operation Center (NOC))	একটি নেটওয়ার্ক নিয়ন্ত্রণ কেন্দ্র (NOC) "নেটওয়ার্ক ম্যানেজমেন্ট সেন্টার" হিসাবেও পরিচিত, এমন এক বা একাধিক অবস্থান যা থেকে কম্পিউটার, টেলিযোগাযোগ বা স্যাটেলাইট নেটওয়ার্কের মাধ্যমে নেটওয়ার্ক মনিটরিং এবং নিয়ন্ত্রণ, বা নেটওয়ার্ক পরিচালনার কাজে ব্যবহার করা হয়।
৮৪	নিরাপত্তা নিয়ন্ত্রণ কেন্দ্র (Security Operation Center (SOC))	সিকিউরিটি অপারেশন সেন্টার (SOC) একটি কেন্দ্রীয় ইউনিট যা সাংগঠনিক এবং প্রযুক্তিগত স্তরের সুরক্ষার বিষয়গুলি নিয়ে কাজ করে। কোনও বিল্ডিং বা স্থাপনার মধ্যে এসওসি একটি কেন্দ্রীয় অবস্থান যেখানে থেকে কর্মীরা ডেটা প্রসেসিং প্রযুক্তি ব্যবহার করে সাইটটি তদারকি করে।
৮৫	প্রধান আর্থিক কর্মকর্তা	প্রধান আর্থিক কর্মকর্তা (CFO) হলেন কোনও সংস্থার আর্থিক কার্যকলাপ পরিচালনার জন্য দায়িত্বপ্রাপ্ত সিনিয়র এক্সিকিউটিভ। সিএফওর দায়িত্বের মধ্যে নগদ প্রবাহ এবং আর্থিক

	(CFO)	পরিকল্পনার পাশাপাশি কোম্পানির আর্থিক শক্তি এবং দুর্বলতাগুলি বিশ্লেষণ করা এবং সংশোধনমূলক পদক্ষেপের প্রস্তাব দেওয়া অন্তর্ভুক্ত।
৮৬	প্রধান তথ্য কর্মকর্তা (CIO)	প্রধান তথ্য কর্মকর্তা (CIO), প্রধান ডিজিটাল অফিসার বা ইনফরমেশন টেকনোলজির ডিরেক্টর, এমন একটি কাজের শিরোনাম যা সাধারণত কোনও উদ্যোগের সিনিয়র এক্সিকিউটিভকে দেওয়া হয়, যিনি এন্টারপ্রাইজের লক্ষ্যগুলি সমর্থন করার জন্য তথ্য প্রযুক্তি এবং কম্পিউটার সিস্টেমের সাথে কাজ করেন।
৮৭	প্রধান প্রযুক্তি কর্মকর্তা (CTO)	একজন প্রধান প্রযুক্তি কর্মকর্তা (CTO), যা কখনও কখনও প্রধান কারিগরি কর্মকর্তা বা প্রধান প্রযুক্তিবিদ হিসাবেও পরিচিত, কোনও সংস্থা বা অন্য সত্তায় নির্বাহী স্তরের পদ, যার পেশা কোনও সংস্থার মধ্যে বৈজ্ঞানিক এবং প্রযুক্তিগত বিষয়গুলিতে নিবদ্ধ থাকে।
৮৮	প্রধান তথ্য নিরাপত্তা কর্মকর্তা (CISO)	একজন প্রধান তথ্য সুরক্ষা কর্মকর্তা (CISO) হ'ল সংস্থার মধ্যে সিনিয়র পর্যায়ের নির্বাহী যিনি, এন্টারপ্রাইজ দৃষ্টিভঙ্গি, কৌশল এবং প্রোগ্রাম যথাযথভাবে সুরক্ষিত রয়েছে তা নিশ্চিত করার লক্ষ্যে এন্টারপ্রাইজ দৃষ্টিভঙ্গি, কৌশল এবং কর্মসূচী প্রতিষ্ঠা করার জন্য দায়বদ্ধ।
৮৯	ডার্ক ওয়েব (Dark Web)	ডার্ক ওয়েব হল ওয়ার্ল্ড ওয়াইড ওয়েবের (World Wide Web) একটি উপাদান যা ডার্ক নেটে বিদ্যমান। আমরা যে ইন্টারনেট ব্যবহার করি সেটা মাত্র পাঁচ থেকে ছয় শতাংশ। এটি পাবলিক ইন্টারনেট ব্যবহারকারী একধরনের লুকায়িত নেটওয়ার্ক। এতে প্রবেশ করতে নির্দিষ্ট সফটওয়্যার, কনফিগারেশন বা অনুমোদনের প্রয়োজন হয়। ডার্ক ওয়েব মূলত ডিপ ওয়েবের একটি অংশ। এই অংশে সাধারন সার্চ ইঞ্জিন প্রবেশ করতে পারে না। যদিও কখনও কখনও ভুল করে "ডিপ ওয়েব" শব্দটি ডার্ক ওয়েবকে বোঝাতে ব্যবহার করা হয়।

পরিশিষ্ট-ক

Audit Checklist – ISO 27001 Framework

Master Control Sections	Master Control Objective	Control Sub-category	Control Sub-category Objectives
A.5.1 Information security policy	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	A.5.1.1 Information security policy document	An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties.
		A.5.1.2 Review of the information security policy	The information security policy shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
A.6.1 Internal organization	Objective: To manage information security within the organization.	A.6.1.1 Management commitment to information security	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
		A.6.1.2 Information security coordination	Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions.
		A.6.1.3 Allocation of information security responsibilities	All information security responsibilities shall be clearly defined.
		A.6.1.4 Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be defined and implemented.
		A.6.1.5 Confidentiality agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
		A.6.1.6 Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.
		A.6.1.7 Contact with special interest groups	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

		A.6.1.8 Independent review of information security	The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
A.6.2 External parties	To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.	A.6.2.1 Identification of risks related to external parties	The risks to the organization's information and information processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
		A.6.2.2 Addressing security when dealing with customers	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
		A.6.2.3 Addressing security in third party agreements	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.
A.7.1 Responsibility for assets	To achieve and maintain appropriate protection of organizational assets.	A.7.1.1 Inventory of assets	All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.
		A.7.1.2 Ownership of assets	All information and assets associated with information processing facilities shall be 'owned' by a designated part of the organization.
		A.7.1.3 Acceptable use of assets	Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.
A.7.2 Information classification	To ensure that information receives an appropriate level of protection.	A.7.2.1 Classification guidelines	Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the organization.
		A.7.2.2 Information labelling and handling	An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
A.8.1 Prior to employment	To ensure that employees, contractors and third party users understand their responsibilities, and are	A.8.1.1 Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security

	suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.	A.8.1.2 Screening	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
		A.8.1.3 Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall state their and the organization's responsibilities for information security.
A.8.2 During employment	To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.	A.8.2.1 Management responsibilities	Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.
		A.8.2.2 Information security awareness, education and training	All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
		A.8.2.3 Disciplinary process	There shall be a formal disciplinary process for employees who have committed a security breach.
A.8.3 Termination or change of employment	To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.	A.8.3.1 Termination responsibilities	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
		A.8.3.2 Return of assets	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
		A.8.3.3 Removal of access rights	The access rights of all employees, contractors and third party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.
A.9.1 Secure areas	To prevent unauthorized physical access, damage and interference to the organization's premises and information.	A.9.1.1 Physical security perimeter	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.
		A.9.1.2 Physical entry controls	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.
		A.9.1.3 Securing offices, rooms and facilities	Physical security for offices, rooms, and facilities shall be designed and applied
		A.9.1.4 Protecting against external and environmental threats	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.

		A.9.1.5 Working in secure areas	Physical protection and guidelines for working in secure areas shall be designed and applied.
		A.9.1.6 Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
A.9.2 Equipment security	To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.	A.9.2.1 Equipment siting and protection	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
		A.9.2.2 Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
		A.9.2.3 Cabling security	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
		A.9.2.4 Equipment maintenance	Equipment shall be correctly maintained to ensure its continued availability and integrity.
		A.9.2.5 Security of equipment off premises	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
		A.9.2.6 Secure disposal or re-use of equipment	All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
		A.9.2.7 Removal of property	Equipment, information or software shall not be taken off-site without prior authorization.
A.10.1 Operational procedures and responsibilities	To ensure the correct and secure operation of information processing facilities.	A.10.1.1 Documented operating procedures	Operating procedures shall be documented, maintained, and made available to all users who need them.
		A.10.1.2 Change management	Changes to information processing facilities and systems shall be controlled.
		A.10.1.3 Segregation of duties	Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.
		A.10.1.4 Separation of development, test and operational facilities	Development, test and operational facilities shall be separated to reduce the risks of unauthorized access or changes to the operational system.
A.10.2 Third party service delivery management	To implement and maintain the appropriate level of information security and service delivery in line with	A.10.2.1 Service delivery	It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

	third party service delivery agreements.	A.10.2.2 Monitoring and review of third party services	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.
		A.10.2.3 Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
A.10.3 System planning and acceptance	To minimize the risk of systems failures.	A.10.3.1 Capacity management	The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
		A.10.3.2 System acceptance	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
A.10.4 Protection against malicious and mobile code	To protect the integrity of software and information.	A.10.4.1 Controls against malicious code	Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
		A.10.4.2 Controls against mobile code	Where the use of mobile code is authorized, the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code shall be prevented from executing.
A.10.5 Back-up	To maintain the integrity and availability of information and information processing facilities.	A.10.5.1 Information back-up	Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.
A.10.6 Network security management	To ensure the protection of information in networks and the protection of the supporting infrastructure.	A.10.6.1 Network controls	Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
		A.10.6.2 Security of network services	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.
A.10.7 Media handling	To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.	A.10.7.1 Management of removable media	There shall be procedures in place for the management of removable media.
		A.10.7.2 Disposal of media	Media shall be disposed of securely and safely when no longer required, using formal procedures.

		A.10.7.3 Information handling procedures	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse.
		A.10.7.4 Security of system documentation	System documentation shall be protected against unauthorized access.
A.10.8 Exchange of information	To maintain the security of information and software exchanged within an organization and with any external entity.	A.10.8.1 Information exchange policies and procedures	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.
		A.10.8.2 Exchange agreements	Agreements shall be established for the exchange of information and software between the organization and external parties.
		A.10.8.3 Physical media in transit	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.
		A.10.8.4 Electronic messaging	Information involved in electronic messaging shall be appropriately protected.
		A.10.8.5 Business information systems	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
A.10.9 Electronic commerce services	To ensure the security of electronic commerce services, and their secure use.	A.10.9.1 Electronic commerce	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.
		A.10.9.2 On-line transactions	Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
		A.10.9.3 Publicly available information	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
A.10.10 Monitoring	To detect unauthorized information processing activities.	A.10.10.1 Audit logging	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

		A.10.10.2 Monitoring system use	Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.
		A.10.10.3 Protection of log information	Logging facilities and log information shall be protected against tampering and unauthorized access.
		A.10.10.4 Administrator and operator logs	System administrator and system operator activities shall be logged.
		A.10.10.5 Fault logging	Faults shall be logged, analyzed, and appropriate action taken.
		A.10.10.6 Clock synchronization	The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.
A.11.1 Business requirement for access control	To control access to information.	A.11.1.1 Access control policy	An access control policy shall be established, documented, and reviewed based on business and security requirements for access.
A.11.2 User access management	To ensure authorized user access and to prevent unauthorized access to information systems.	A.11.2.1 User registration	There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.
		A.11.2.2 Privilege management	The allocation and use of privileges shall be restricted and controlled.
		A.11.2.3 User password management	The allocation of passwords shall be controlled through a formal management process.
		A.11.2.4 Review of user access rights	Management shall review users' access rights at regular intervals using a formal process.
A.11.3 User responsibilities	To prevent unauthorized user access, and compromise or theft of information and information processing facilities	A.11.3.1 Password use	Users shall be required to follow good security practices in the selection and use of passwords.
		A.11.3.2 Unattended user equipment	Users shall ensure that unattended equipment has appropriate protection.
		A.11.3.3 Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.
A.11.4 Network access control	To prevent unauthorized access to networked services.	A.11.4.1 Policy on use of network services	Users shall only be provided with access to the services that they have been specifically authorized to use.

		A.11.4.2 User authentication for external connections	Appropriate authentication methods shall be used to control access by remote users.
		A.11.4.3 Equipment identification in networks	Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.
		A.11.4.4 Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports shall be controlled.
		A.11.4.5 Segregation in networks	Groups of information services, users, and information systems shall be segregated on networks.
		A.11.4.6 Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications
		A.11.4.7 Network routing control	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
A.11.5 Operating system access control	To prevent unauthorized access to operating systems.	A.11.5.1 Secure log-on procedures	Access to operating systems shall be controlled by a secure log-on procedure.
		A.11.5.2 User identification and authentication	All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.
		A.11.5.3 Password management system	Systems for managing passwords shall be interactive and shall ensure quality passwords.
		A.11.5.4 Use of system utilities	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
		A.11.5.5 Session time-out	Inactive sessions shall shut down after a defined period of inactivity.
		A.11.5.6 Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.
A.11.6 Application and information access control	To prevent unauthorized access to information held in application systems.	A.11.6.1 Information access restriction	Access to information and application system functions by users and support personnel shall be restricted in accordance with the defined access control policy.
		A.11.6.2 Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment.

A.11.7 Mobile computing and teleworking	To ensure information security when using mobile computing and teleworking facilities.	A.11.7.1 Mobile computing and communications	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication facilities.
		A.11.7.2 Teleworking	A policy, operational plans and procedures shall be developed and implemented for teleworking activities.
A.12.1 Security requirements of information systems	To ensure that security is an integral part of information systems.	A.12.1.1 Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.
A.12.2 Correct processing in applications	To prevent errors, loss, unauthorized modification or misuse of information in applications.	A.12.2.1 Input data validation	Data input to applications shall be validated to ensure that this data is correct and appropriate.
		A.12.2.2 Control of internal processing	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
		A.12.2.3 Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.
		A.12.2.4 Output data validation	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
A.12.3 Cryptographic controls	To protect the confidentiality, authenticity or integrity of information by cryptographic means.	A.12.3.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
		A.12.3.2 Key management	Key management shall be in place to support the organization's use of cryptographic techniques.
A.12.4 Security of system files	To ensure the security of system files.	A.12.4.1 Control of operational software	There shall be procedures in place to control the installation of software on operational systems.
		A.12.4.2 Protection of system test data	Test data shall be selected carefully, and protected and controlled.
		A.12.4.3 Access control to program source code	Access to program source code shall be restricted.
A.12.5 Security in development	To maintain the security of application system software and	A.12.5.1 Change control procedures	The implementation of changes shall be controlled by the use of formal change control procedures.

and support processes	information.	A.12.5.2 Technical review of applications after operating system changes	When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.
		A.12.5.3 Restrictions on changes to software packages	Modifications to software packages shall be discouraged, limited to necessary changes, and all changes shall be strictly controlled.
		A.12.5.4 Information leakage	Opportunities for information leakage shall be prevented.
		A.12.5.5 Outsourced software development	Outsourced software development shall be supervised and monitored by the organization.
A.12.6 Technical Vulnerability Management	To reduce risks resulting from exploitation of published technical vulnerabilities.	A.12.6.1 Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used shall be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.
A.13.1 Reporting information security events and weaknesses	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	A.13.1.1 Reporting information security events	Information security events shall be reported through appropriate management channels as quickly as possible.
		A.13.1.2 Reporting security weaknesses	All employees, contractors and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
A.13.2 Management of information security incidents and improvements	To ensure a consistent and effective approach is applied to the management of information security incidents.	A.13.2.1 Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.
		A.13.2.2 Learning from information security incidents	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
		A.13.2.3 Collection of evidence	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).
A.14.1 Information security aspects of business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure	A.14.1.1 Including information security in the business continuity management process	A managed process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

	their timely resumption.		
		A.14.1.2 Business continuity and risk assessment	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
		A.14.1.3 Developing and implementing continuity plans including information security	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.
		A.14.1.4 Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
		A.14.1.5 Testing, maintaining and reassessing business continuity plans	Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.
A.15.1 Compliance with legal requirements	To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.	A.15.1.1 Identification of applicable legislation	All relevant statutory, regulatory and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
		A.15.1.2 Intellectual property rights (IPR)	Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
		A.15.1.3 Protection of organizational records	Important records shall be protected from loss, destruction and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
		A.15.1.4 Data protection and privacy of personal information	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.
		A.15.1.5 Prevention of misuse of information processing facilities	Users shall be deterred from using information processing facilities for unauthorized purposes.
		A.15.1.6 Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
A.15.2 Compliance with security policies and standards, and technical	To ensure compliance of systems with organizational security policies and standards.	A.15.2.1 Compliance with security policies and standards	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

compliance		A.15.2.2 Technical compliance checking	Information systems shall be regularly checked for compliance with security implementation standards.
A.15.3 Information systems audit considerations	To maximize the effectiveness of and to minimize interference to/from the information systems audit process.	A.15.3.1 Information systems audit controls	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimize the risk of disruptions to business processes.
		A.15.3.2 Protection of information systems audit tools	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

পরিশিষ্ট-খ

Audit Checklist – ISO 27005 Framework

Master Control Sections	Master Control Objective	Control Sub-category	Control Sub-category Objectives
A 8 Risk assessment	Identification and valuation of assets and impact assessments	8.1 Risk identification	8.1.1 Identification of assets
			8.1.2 Identification of threats
			8.1.3 Identification of existing controls
			8.1.4 Identification of vulnerabilities
			8.1.5 Identification of consequences
		8.2 Risk analysis	PILAR evaluates the risk associated to each threat on each asset, and provides a risk-level that is a combination of the likelihood and the consequences of the occurrence of each threat on each asset.
		8.3 Risk evaluation	PILAR provides detailed information on the facts. It is the responsibility of the management bodies to interpret the consequences of incidents on the business.
A 9 Risk treatment	Risk treatment is an art where organization may opt between several, non-exclusive, alternatives	9.1 Risk Modification	The level of risk should be managed by introducing, removing or altering controls so that the residual risk can be reassessed as being acceptable
		9.2 Risk Retention	The decision on retaining the risk without further action should be taken depending on risk evaluation.

		9.3 Risk Avoidance	The activity or condition that gives rise to the particular risk should be avoided. Usually this means changing the collection of assets, removing from our system those that we are not ready to protect sufficiently.
		9.4 Risk Sharing	The risk should be shared with another party that can most effectively manage the particular risk depending on risk evaluation

A 10 Risk acceptance	PILAR provides detailed information on the facts, both potential and residual risk levels. It is the responsibility of the management bodies to take the decisions.		
A 11 Risk communication	Risk communication is an activity to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decision-makers and other stakeholders. The information includes, but is not limited to the existence, nature, form, likelihood, severity, treatment, and acceptability of risks		
A 12 Risk monitoring	Risks are not static. Threats, vulnerabilities, likelihood or consequences may change abruptly		

পরিশিষ্ট-গ

Audit Checklist – ISO 27001 Framework

S No	Data Center and Near Data Center Controls
1	**Physical Security**
1.1	Is physical security applied to the information processing area or DC/NDC and unauthorized access strictly prohibited
1.2	Does BCC limit access to DC/NDC to authorized staff only
1.3	Is there any access authorization procedure in place to ensure that vendors, service providers, support staff, cleaning crews, etc visitors are accompanied at all times by an authorized employee while in the DC/NDC and the whole procedure should be abide by vendor access policy

1.4	Is access authorization list with and/or without biometric profile maintained and reviewed periodically for the authorized person to access the DC/NDC
1.5	Are all physical access to sensitive areas logged with date, time and purpose
1.6	Does the management ensure and monitor physical security of the perimeter of DC, facility and equipment room by employing physical and procedural controls for 24 hours
1.7	Is emergency exit door available
1.8	Is there a designated custodian or manager in charge of DC/NDC to provide authorization and to ensure compliance with policy
1.9	Is there an inventory of all computing equipment, associated equipment and consumables housed in DC/NDC and gate pass policy should be in place during movement of any asset
1.10	Is there enough checkpoints including metal detector in place to ensure proper approval from the competent authority before entering or exiting any equipment or accessories into/from the DC/NDC
1.11	Is lost access card reported immediately as occurrence of incident and then access on lost card immediately revoked
1.12	Is the physical security of DC/NDC premises reviewed at least once each year
1.13	Is there enough checkpoints in place to ensure proper approval from the competent authority before entering or exiting any equipment or accessories into/from the DC/NDC
2	**Environmental Security**
2.1	Is the DC/NDC designed and applied to protect from the risk of damage due to fire, flood, explosion and other forms of disaster
2.2	Is design layout of DC/NDC including power supply and network connectivity properly documented and approved
2.3	Are there separate channels for data and power cables to protect from interception or any sort of damages
2.4	Are water detection devices placed below the raised floor if it is raised
2.5	Is there any pest control mechanism in place
2.6	Is there any storage of accessories or devices not associated with DC and powered off devices including phone, laptop or any accessories that has camera which are disallowed in the DC/NDC and must be blocked by sticker
2.7	Is Close Circuit Television (CCTV) camera installed at appropriate positions of all sides for monitoring
2.8	Is there any sign of "No eating, drinking or smoking", "Fire, power cutoff, Accident etc." in display
2.9	Is there any dedicated office vehicle for emergency necessities
2.10	Does the data centers have dedicated telephone communication facility
2.11	Are the addresses and telephone or mobile numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT personnel) available to meet any emergency necessity
2.12	Are power supply system and other support units separated from production site and placed in secure area to reduce the risks from environmental threats

2.13	Is dedicated power supply installed from source (MDB or Generator) to DC/NDC and monitored to avoid the risk of overloading
2.14	Are the following environmental controls installed: a) Uninterrupted Power Supply (UPS) with backup units b) Backup power supply c) Estimated necessary fuel for generator(s) d) Temperature and humidity measuring devices e) Water leakage precautions and water drainage system from air conditioner f) Air conditioners with backup units. Industry standard cooling system shall be introduced to avoid the water leakage and faults in the water drainage system with the conventional air conditioning system g) Emergency power cut-off switches where applicable h) Emergency lighting arrangement i) Dehumidifier for humidity control
2.15	Is First-Aid kit kept available in both DC/NDC
2.16	Is any photograph taken inside the DC by any staffs should be monitored and blocked by sticker
2.17	Are all above mentioned controls regularly tested and existence of maintenance service contract available for 24x7 bases
3	**Fire Prevention**
3.1	Are wall, ceiling and door of DC/NDC fire-resistant
3.2	Are fire suppression equipment installed and tested periodically
3.3	Is automatic fire/smoke alarming system installed and tested periodically
3.4	Is there fire detector below the raised floor if it is raised
3.5	Are electric cables and data cables in the DC/NDC maintained quality and concealed
3.6	Are flammable items e.g. paper, wooden items, plastics, etc. allowed to store in the DC
4	**Server Room Controls**
4.1	Is there a glass enclosure in the server room with lock and key under a responsible person
4.2	Is the physical access restricted and visitors' log maintained for the server room
4.3	Is there any access authorization list which is being maintained and reviewed on regular basis
4.4	Is there any provision to replace the server and network devices within shortest possible time in case of any disaster
4.5	Is the server room air-conditioned and installed with proper water drainage system
4.6	Is there power generator in place to continue operations in case of power failure
4.7	Is there UPS in place to provide uninterrupted power supply to the server and devices
4.8	Is proper attention given on overloading electrical outlets with too many devices
4.9	Is channel alongside the wall prepared to allow all required cabling to be in neat and safe position as per layout of power supply and data cables

4.10	Are the addresses and phone numbers of all contact persons (e.g. fire service, police station, service providers, vendors and all ICT/ responsible personnel) available to cope with any emergency situation
4.11	Is power supply switched off before leaving the server room if otherwise not required
4.12	Is fire extinguisher placed outdoor visible area of the server room and maintained/checked on an annual basis
4.13	Is there enough checkpoints in place to ensure proper approval from the competent authority before entering or exiting any equipment or accessories into/from Server Room
5	**Networks Security Management**
5.1	Is there any standard established to ensure security for OSs, Databases, Network equipments and portable devices
5.2	Are enforcement checks conducted regularly to ensure that the standards are applied uniformly and non-compliances are detected and raised for investigation
5.3	Are the Network Design and its security configurations implemented under an approved documented plan
5.4	Are all type of cables including UTP, fiber, power labeled properly for further corrective or preventive maintenance works
5.5	Is physical security of all network equipment ensured
5.6	Are groups of information services, users, and information systems segregated in networks, e.g. VLAN
5.7	Are unauthorized access and electronic tampering controlled strictly, and encryption mechanism deployed for sensitive data travelling through public network
5.8	Are network security devices e.g. Firewall, IDS, IPS installed to protect the network perimeters
5.9	Is web Application Firewall (WAF) implemented to protect hosted web applications
5.10	Are there firewalls or other security measures deployed within internal networks to minimize the impact of security exposures
5.11	Is Secure Login feature (i.e. SSH) enabled and unencrypted login option (i.e. TELNET) disabled in network devices for remote administration purposes
5.12	Are rules on network security devices backed up and reviewed on a regular basis
5.13	Is there any arrangement of redundant communication links for WAN connectivity
5.14	Are all unused ports of network devices e.g. switch, router, etc. shut-off by default if otherwise not defined
5.15	Is network extension using Hub, Wireless Router (WiFi), etc. prohibited
5.16	Is network extension for new users done centrally with approval from authority
5.17	Is connection of personal laptop to office network or any personal wireless modem with the office laptop/desktop restricted and secured
5.18	Is SYSLOG server established to monitor the logs generated by network devices (depending on Network Size)
5.19	Is Authentication Authorization and Accounting (AAA) Server established to manage the network devices effectively (depending on Network Size)

5.20	Are Role-based and/or Time-based ACLs implemented in the routers to control network traffic
5.21	Is real time health monitoring system implemented for surveillance of all network equipments and servers
5.22	Are all default passwords of network devices changed immediately after installation
5.23	Are all communication devices uniquely identifiable with proper authentication
5.24	Is role-based administration ensured for the servers and network devices
5.25	Is configuration backup of the network devices done regularly
5.26	Are control and visibility of the network with technology e.g. NetFlow, sFlow, etc. in place
5.27	Is Rollback policy for system update/Upgrade/Configuration management available
5.28	Is Configuration Management Database (CMDB) implemented and reviewed regularly
5.29	Is all documents related to Configuration, Change, Incident, Problem and Root Cause Analysis (RCA) stored
5.30	Is white list-based network traffic policy implemented
6	**Malicious Code Protection**
6.1	Are the servers and workstations protected from malicious code by ensuring the proper installation of approved anti-malware packages
6.2	Are the users aware of prevention and detection of the introduction of malicious software
6.3	Are software and data supporting critical business activities regularly scanned or searched to identify possible malicious code
6.4	Are the files received on electronic media of uncertain origin or unknown networks checked for malicious code before use
6.5	Are attachments of electronic mail checked for malicious code before use
6.6	Is the anti-malware package kept up-to-date with the latest definition file using an automated and timely process
6.7	Are all computers in the network get updated signature of anti-malware software automatically from the server
6.8	Is auto protection mode enabled to screen disks, tapes, CDs or other media for malwares
6.9	Are the employees made aware of the problem of hoax viruses and advised not to forward such chain mail to others
6.10	Is there any formal process for managing attacks from malicious code including reporting of and recovering from attacks
6.11	Is there any Sandboxing mechanism for further malware analysis
6.12	Is awareness program arranged for the end users about computer malwares and their prevention mechanism
7	**Internet Access Management**
7.1	Are access to and use of the internet from BCC's premises kept secure
7.2	Is access to the Internet from BCC premises and systems routed through secure gateways

7.3	Is external internet connectivity device prohibited to be used in the BCC's resources at BCC premises
7.4	Is internet access provided by BCC prohibited to transact any commercial/business activity that is not done by the BCC
7.5	Are critical internal workstations for financial transactions isolated from the network having internet
7.6	Is there any procedure of disciplinary action for the case of activity that knowingly contravenes any criminal or civil law or act using internet access provided by BCC
7.7	Is formal risk analysis performed during deployment of connections to the Internet or third-party and public networks
7.8	Is there any white-listing and/or black-listing policy developed and maintained
7.9	Is visibility of the users' internet access in place
8	**Email Management**
8.1	Is email system maintained according to BCC's E-mail Policy
8.2	Is encryption facility used while confidential information communicated to external parties
8.3	Are employees compelled to consider the confidentiality and sensitivity of all email content, before forwarding email or replying to external parties
8.4	Is there any procedure of disciplinary action for information transmitted by email which are defamatory, abusive, involve any form of racial or sexual abuse, damage the reputation or contain any material that is harmful to employees, customers, competitors, or others
8.5	Does BCC restrict personal usage of BCC's email address for any social networking, blogs, groups, forums, etc.
8.6	Is there any mechanism in place to restrict and control inbound email sourcing of any social networking, blogs, groups, forums, etc.
8.7	Do the employees use a disclaimer stating about confidentiality of email contents and asking intended recipient for transmission
8.8	Are regular review and monitoring of email services performed by concerned department
9	**Cryptography**
9.1	Is there any established cryptographic key management policy and procedure to cover generation, distribution, installation, renewal, revocation and expiry
9.2	Are all cryptographic keys generated securely and materials used in the generation process destroyed after usage
9.3	Are cryptographic keys used for a single purpose to reduce the impact of an exposure of a key
9.4	Is there defined cryptoperiod for each cryptographic key considering sensitivity and operational criticality
9.5	Are the hardware security modules and keying materials physically and logically protected
9.6	Is use or transmission of cryptographic keys are secured
9.7	Is there any secure key destruction method for expired cryptographic keys

9.8	Is the generation of a new key independent from the previous keys
9.9	Is backup of cryptographic keys maintained
9.10	Is there any procedure in place for key revocation/destruction/replacement of the compromised keys
10	**Vulnerability Assessment and Penetration Testing**
10.1	Are VAs conducted regularly to detect security vulnerabilities in the ICT infrastructure and applications
10.2	Is there any procedure for combination of automated tools and manual techniques to perform comprehensive VA
10.3	Is there any process in place to remedy issues identified in VAs and perform subsequent remediation of gaps
10.4	Are periodical or need basis penetration tests conducted on network infrastructure and internet-based systems
10.5	Is periodical VAPT conducted on total infrastructure and web-based systems
11	**Patch Management**
11.1	Is there any patch management procedure to identify, categorize, prioritize and implement patches in a timely manner
11.2	Are patches deployed in test environment before deployment into the production environment
11.3	Are License management policy in place
12	**Security Monitoring**
12.1	Are there appropriate security monitoring systems and processes in place to facilitate prompt detection of unauthorized or malicious activities by internal and external parties
12.2	Are network surveillance and security monitoring procedures implemented to protect BCC against network intrusion attacks
12.3	Are security monitoring tools implemented to enable the detection of changes on critical ICT resources such as databases, system or data files and programs, to facilitate the identification of unauthorized changes
12.4	Are security logs of systems, applications and network devices regularly reviewed for anomalies, and logs being protected for a defined period