DATA CENTER & SERVER ROOM DESIGN

Imagine Technology Pvt. Ltd.

Jayceesmarg, Thapathali, Kathmandu

Tel : 01-4245501, 01-4245701

sales@imagineit.com.np | www.imagineit.com.np

Data Center & Server Room Design

INTRODUCTION

The server room primarily serves to accommodate servers & network hardware, e.g. a LAN or application server(s), Server host computer(s), mid range host(s) etc. In addition, additional hardware such as an air conditioning system, other sensors may be kept in that room.

Regular staff shall normally not occupy a server room, it will be used only sporadically and for short term assignments.

DATA CENTER FUNCTION

1. To provide a safe and secure place to locate mission critical equipment.
2. To provide sufficient power protection to maintain the critical load.
3. To provide communications connectivity both inside and outside the Organization.

DATA CENTER PHILOSOPHY

The goal of any data center is to provide continuous availability of all hardware & network services. Therefore, while planning for datacenter the overall philosophy remains the same for large as well as small datacenter.

- Keep it as simple as possible
- Design for scalability
- Utilize modularity wherever possible
- Be flexible and adaptable to change

DATA CENTER CONSTRUCTION GUIDELINES

A – Server Room Construction

- Specify the minimum clearance or room height (Min. 7.5 ft from Finished Floor, After Raised Flooring)
- Specify the size. Note there are minimum sizes based on the square footage of the facility depending upon the density of Servers & Racks.

- Specify that there shall be Fire Resistant Acoustic Modular false ceiling where required.
- Specify minimum door opening (Min. 5 ft)
- It is highly recommended that the door enter from the Hall.
- Specify the use of Anti Static Raised Flooring or static free flooring.
- Specify the provision of a lock to restrict access. (Electronic/Biometric & Manual)

B – Server Room Environment Control

- HVAC to provide constant temperature and humidity control in degrees (C) and the Relative Humidity (RH) based on the standards for active or passive components. (Temp between 12 to 18 degree C & Humidity between 20 to 50 %)
- Specify the minimum number of air changes per hour to reduce dust.
- HVAC Device must be dedicated for the Data Center, building HVAC system shall not be used.
- Need for a secondary/redundant cooling system and/or temperature alarm system.

C – Server Room Fire Suppression Concerns

- FM-200 based Automatic Fire Suppression system is recommended.
- Two coats fire retardant white paint on walls and /or drywall over plywood
- Fire stop all sleeves and conduit

D – Flooding

- Location to be high and dry or racks curbed to prevent flood damage
- No penetration through ceiling or water sources above
- Water Leak Detection shall be used under the Raised Flooring & Nearby HVAC device.

E – Lighting

- Specify the Min Ft candles @ 1 meter AFF as per the BICSI standard
- Emergency lighting powered by UPS shall be used.

F – Electrical

- Branch circuits be 20A
- Grounding All equipment and cables grounded
- Floor grounding is required if anti-static Raised Flooring is used.
- Specify dedicated power panel for the room and HVAC device
- Separate convenience electrical for power tools at set intervals around room
- Convenience power be visibly marked
- Data power minimum 2 duplex plugs 3 wire 220vac, additional as per spec and room expectations
- All Cabling i.e. Under Flooring & Overhead must be runned through Cable Trays.

DATA CENTER THREAT SCENARIO

The following threats are assumed as regards to the IT baseline protection of a server room:

Fire

Apart from direct fire causing damage to a building or its equipment, there may be consequential damage, the impact of which can, especially for IT systems, assume disastrous dimensions.

Not only negligent handling of combustible material causes a fire, but also by improper use of electric devices.
The following, amongst others, can facilitate spreading of a fire:

- The improper storage of combustible material.
- The lack of fire detection devices.
- Insufficient fire protection (e.g. lack of fire insulation along cable routes).

Water

The uncontrolled flow of water into buildings or rooms may, for instance, result from:

- Rain, floods, inundation;
- Disruption of water supply and sewerage systems;
- Defects of the HVAC system;
- Defects of sprinkler systems; and
- Water used for fire fighting.

No matter how water will get into buildings or rooms, the danger is that it will damage, or make inoperable supply facilities or IT components (short circuit, mechanical damage, rust, etc.). Where central supplies for the building are accommodated (main power distributor, trunk distribution frame for telephone, data) in basement rooms without automatic water removal, ingress of water can cause considerable damage.

Inadmissible temperature and humidity

Every device has a temperature range within which its proper functioning is ensured. If the room temperature exceeds the limits of that range in either direction, discontinuity of service and failure of devices may result.

In a server room, for instance, the devices accommodated there will generate electric power and thus heat up the room. If ventilation is insufficient, the admissible operating temperature of the devices may be exceeded. In case of solar radiation, room temperatures of more than 50° C are not improbable.

Organizational shortcomings

Lack of or insufficient rules

The importance of organizational regulations and requirements for IT security objectives increases with both the information processing volume and the protection requirement of the information to be processed.

Insufficient knowledge of rules

Determining rules alone does not guarantee smooth IT operations. That people concerned must know what rules apply to a certain instance.

Unauthorized access to rooms requiring protection

If unauthorized persons enter protected rooms, hazards may be entailed not only by deliberate acts, but also by inadvertence. Disruption is caused merely by the fact that checks must be made for potential damage as a result of the unauthorized access.

Technical Failure

Disruption of power supply

Despite high assurance of supply continuity, power supply by utilities will be disrupted from time to time. For the major part, such failures, with duration of less than one second, are so short that people will not notice them. But IT operations can be disrupted even by failures of less than 10ms. These interruptions were exclusively due to failures of the supply network. In addition, interruptions may be caused by disconnection for unannounced maintenance/repair purposes or by cables damaged during below grade construction.

Not only the obvious, direct power consumers (PC, lighting, etc.) depend on power supply. All infrastructure installations are nowadays directly or indirectly dependent on electric power, for instance: elevators, pneumatic dispatch systems, air conditioning, intruder and fire detection devices, telephone private branch exchanges. Even water supplies in high rise buildings are current dependent on account of the pumps needed for pressure in the upper storeys.

Failure of internal supplies

In a building a variety of utilities exists for supply and disposal and thus serves as a basis for IT processes. For instance, the failure of the electricity, telephone system, and the air conditioning/ventilation system can lead to immediate stoppage of the IT operation. Disruption can also be caused by failure in the following areas:

- Heating
- Water
- Sewerage
- Gas
- Reporting and control devices (intruders; fire; control engineering);
- Intercom systems.

The utilities are mutually dependent in varying degrees so that malfunctions in any of them can also have an impact on others.

Voltage variations

Variations in the supply voltage may result in malfunctions and damaging of IT systems. Such variations range from extremely short and minor incidents that have little or no effect on IT systems to complete failure or destructive over voltage. This may be triggered in all sectors of the power supply network, ranging from the utility network to the circuit to which the respective devices are connected.

Deliberate Acts

Manipulation/destruction of IT equipment or accessories

External as well as internal perpetrators may for various reasons (revenge, malevolence, and frustration) try to manipulate or destroy IT equipment, accessories, documents, or the like. Such manipulations can be the more effective, the later they are detected, the greater the offender's knowledge is and the more momentous the impact on a work cycle is. Effects range from unauthorized disclosure of sensitive data to the destruction of data media or IT systems, which may result in considerable down time periods.

Manipulation of data or software

Data or software can be manipulated in various ways: wrong entry of data, changes to access rights, modifying the contents of account information or of correspondence, changes to the operating system software, etc.

A perpetrator can only manipulate data and software to which he has access. The more access rights a person has, the more serious manipulations may be. If such

manipulations are not detected in time, smooth IT operations may be seriously impaired.

Manipulations of data or software can be performed for reasons of revenge or to obtain personal gains or for financial reasons.

Unauthorized entry into a building

Unauthorized entry into a building precedes various threats to IT systems such as theft or manipulation. Therefore, countermeasures will also be effective against the respective consequential threats.
The direct effect of unauthorized entry can be material damage. Windows and doors will be opened by force and damaged in the process; they will have to be repaired or replaced.

Theft

Theft of IT equipment, accessories, software or data constitutes a threat to be taken very seriously. Such theft entails costs for replacement and for restoration of operability and for losses resulting from lack of availability. Moreover, damage can be caused by loss of confidentiality and its sequels.

Vandalism

Vandalism is very similar to an attack, with the difference that vandalism is not purposive and focused but in most instances is an expression of blind rage.

Such acts may be committed by both external perpetrators (e.g. disappointed burglars, demonstrations which have got out of control) and internal perpetrators (e.g. disgruntled employees or staff members under the influence of alcoholic drinks). The actual threat posed by vandalism is more difficult to assess as that posed by an attack since generally vandalism is not motivated by a conscious effort. Personal problems or a bad organization climate may be the underlying causes.

RECOMMENDED COUNTERMEASURES

For the implementation of IT baseline protection, the following baseline safeguards are recommended.

Adapted wiring of circuits

Experience shows that room allocation and the power ratings, for which an electric installation has been laid out, will after some time no longer match the actual situation. Thus, it is essential to review, and where appropriate to adjust, the electric installation

when rooms are to be used for different purposes and when changes and amendments are made to the technical equipment (IT, air conditioning, and lighting).

Re wiring lines may do this, otherwise it may become necessary to re install feeders, lines, distributors, etc.

Fire extinguishers (Automatic/Manual)

Most fires arise from small sources of fire that if detected early enough can be easily kept under control. In offices, in particular, there will be plenty of material to feed the fire and it can spread very quickly. Therefore, immediate fire fighting is to be given a high priority.

Such immediate fire fighting is only possible if there is a provision of Automatic Fire Suppression System of a sufficient number of hands held fire extinguishers of adequate size are available within the building. The aim must be to place them close to areas and rooms requiring protection, e.g. server room(s), technical infrastructure room(s), document archive(s). Dry powder extinguishers For electronically controlled, e.g. computers, CO^2 extinguishers (class "B") will be adequate.

Fire extinguishers must be regularly checked and maintained. Staff members should memories the location of the nearest fire extinguisher. During fire drills, they should be briefed on the use of automatic as well as hand held fire extinguishers.

Room allocation, with due regard to fire loads

Any combustible material brought into a building produces a fire load. It is determined by the quantity and the calorific value of such material. IT equipment and lines constitute a fire load just as furniture, floor covering and curtains do. Maximum fire loads, standardized calorific values, and further information and provisions have been compiled in the DIN 4102 standard. When planning the installation of IT equipment, data carriers etc., the existing fire loads in the same room and in adjacent rooms should be reviewed. The data carrier archive, for example, should not be located near or above a paper storage area.

Intruder and fire detection devices

If an intruder or fire detection device is installed and if it can be expanded at reasonable cost, it should be considered whether, as a minimum, the IT core areas (server room[s], data carrier distribution centre[s], technical infrastructure room[s], etc.) could be included in the monitoring provided by this device. Thus it will be possible to detect threats such as fire, burglary or theft in good time and to initiate safeguards. In order to

maintain the desired level of protection, the intruder/fire detection device should be serviced and tested on a regular basis.

If an intruder/fire detection device is not available or if an existing device cannot be used, local detection devices should be considered as a minimum. These work on a completely independent basis without being connected to any central facility. Alert is given at the site or by means of a simple two wire line (possibly telephone line) located elsewhere.

Avoidance of water pipes

In rooms or areas housing IT facilities with central functions (e.g. server[s]), water pipes of any type should be avoided. Where absolutely necessary, the only water carrying lines installed should be coolant pipes, fire-fighting water pipes and heating pipes. Supply lines to radiators should be furnished with gate valves where possible, outside the room/area. These valves must be shut outside the heating period.

If water pipes cannot be avoided, minimum protection can be provided by water sump or drip pan installed under the pipeline, the drain of which leads outside the room. For this purpose, it is expedient to use the corridor since then any pipe defects can be detected at an earlier time. Optionally, water detectors with automatic solenoid valves can be installed. Such electro valves should be installed outside the room/area and must be de energized.

Over voltage protection

According to the quality and advancement of the external power supply network and the in house power network, over voltage peaks can, depending on the environment (other power consumers) and on the geographical location, be caused in the supply mains by induction or lightning. As a rule, over voltage due to lightning has quite a destructive potential, while that of over voltage due to other causes is only minor. However, all types of over voltage can destroy IT facilities.

The design of elementary protection depends on the existence of external lightning protection. The protective effect of every stage builds on the preceding stage. If one stage is left out, over voltage protection will, in its entirety, become nearly ineffective.

If over voltage protection cannot be ensured throughout the building, it will at least be possible to establish an adequate protective perimeter around important IT facilities (server[s], etc.). In order to minimize potential damage, networks to which multiple devices are connected can, by means of opto couplers or surge arresters, be divided into small sectors protected from each other.

Emergency circuit breakers

Installation of emergency circuit breakers is advisable in rooms where electrical devices are operated in such a way that, for instance, increased fire hazards exist due to the waste heat of such devices, to compact installation of equipment or to the existence of additional fire loads. Activation of an emergency circuit breaker will eliminate a major source of energy for any fire, and as a result, minor fires can go out. In any case, however, the risk posed by voltages will be eliminated during fire fighting operations.

A point to be borne in mind is that local systems for uninterruptible power supply (ups) will, after the external power supply has been switched off, automatically provide for power supply and that the respective devices will remain live. Therefore, when installing an emergency circuit breaker, it must be ensured that also the UPS will be switched off rather than being merely separated from the external power supply.

The emergency circuit breaker should be installed in the room next to the entrance door (possibly with a note, on the outside of the door, indicating the location of the switch) or outside the room, next to its door. In this context, however, it must be borne in mind that such an emergency circuit breaker may, even in the absence of a threat, be activated inadvertently or intentionally.

Air conditioning

In order to ensure the admissible range of the warmed up temperature of IT devices, the normal air exchange and heat transfer in a room sometimes does not suffice so that installation of air conditioning will be required. Its function is, through cooling, to keep the room temperature under the limit preset by the IT systems.

If, in addition, atmospheric humidity requirements exist, the air conditioner through humidifying and dehumidification can also meet these. For this purpose, however, the air conditioner will have to be connected to a water supply line. In order to preserve the protective effect, provisions must be made for regular maintenance of the air conditioning plant.

Uninterruptible power supply (UPS)

With an uninterruptible power supply (UPS), it is possible to bridge a short term power failure or maintain the power supply long enough to allow orderly shutdown of the connected computers.

On line UPS: The UPS is permanently switched between the mains and the power consumers. The entire power supply is always provided through the UPS.

In addition to tiding over a complete breakdown of power supply and under voltage situations, Online UPS can serve to smooth over voltage.

Remote indication of malfunctions

IT equipment and support devices requiring no, or only infrequent, intervention by a human operator are often located in closed and locked rooms (e.g. server room[s]). As a result, malfunctions that, during the initial stage, do not produce an immediate effect, may not be remedied, and have a ripple effect on other mission critical equipment and systems.

Remote detection provides for earlier discovery of such malfunctions.

IN CONCLUSION

The IT Utility service is one of our core business offerings within the IT related communications and building infrastructure provisioning, deployment and support areas.

Due to the extensive scope, customer expectations and the enormous configuration variables it is not possible to provide a generic or a workable planning blue print: it is a thoroughly planned service that includes value measurement and benchmarking through a site(s) comprehensive assessment exercise to establish the required proof of concept, validate pricing, prove the value of the service, and drive the service improvement mechanism.

Through the site assessment exercise we will, amongst others, determine:

- The realistic threats facing the system(s), ranking the threats in order of significance.
- Thoroughly examining the countermeasures that are deployed and their effectiveness to block the discovered threats.
- Compare the cost of the countermeasures with the value they would bring to the overall security of the system(s).
- Propose additional measures or enhancements to existing measures if deemed necessary.

As part of the site assessment exercise we particularly analyze the environment in terms of power supply and quality, air conditioning and ventilation requirements, fire and intrusion detection mechanisms, physical security and gas suppression and sprinkler systems.

Where necessary we will propose additional measures or enhancements to existing measures.
The information gathered through this process will provide the information required to develop a realistic Site Management and Maintenance Plan that addresses the specific and unique requirements of a particular environment.