

Server Room Installation Project Plan

Prepared

September 26, 2013

For

DMACC Enterprises
2006 Ankeny Blvd.
Ankeny, IA

By



K.O. the Competition. Biz Like a Champ.

Logo concept by Shenica Graham, Booking "Glove from Tearing Paper" by Nr253 at freedigitalphotos.net

Ankeny, IA

The Rock e Tech Team

Shenica Graham (Project Manager)
Brent Leistner
Christopher Mullenberg
Dung Phan

Executive Summary

“Rock e Tech” (pronounced Rocky Teck) is Iowa’s number one information technology designer. Our motto is, “K.O. (knockout) the competition. Biz (do business) like a champ.” Collectively, we have over twenty years of professional experience providing quality information security and management services. Our state of the art equipment and versatile solutions are designed to increase your organization’s productivity without breaking your budget. Our professional team is your key to success in the digital age.

Having a common understanding of the project scope is important to meeting the customer’s needs. For this reason, we provide the following definition of a “server room.” A Rock e Tech server room is a space solely dedicated to housing technology equipment and its supporting infrastructure at an existing location. This multi-use location is expected to function in capacities beyond server housing. Since spaces are unique, there is no one-size fits all design. We will develop an installation tailored to the unique logistics of the customer’s location. We will follow best practices and design a solution to meet the organization’s specific needs as set forth in the request for proposals (RFP).

We will delineate important factors in the areas of requirement definition and building system considerations. Defining the requirements includes consideration for load density, resiliency, growth, modularity, and flexibility. Regarding specific building systems, we will consider the physical space, mechanical systems, electrical systems, and ancillary systems. To find the “best fit” for the customer, we offer pre-installation analysis to identify any preliminary issues that need solving prior to installation. After the server room is installed and configured, our quality service department is Online 24/7 for customer support whenever needed.

This project plan outlines the scope of our intended bid for service and is intended as an outline, not an absolute. Additional elements may be compiled as necessary, to develop the most comprehensive, contract-winning bid.

The Rock e Tech Team

Your Rock e Tech Server Room design team includes the following key leaders

- **Shenica Graham.** Ms. Graham is your Server Room design Project Manager. She will be your point of contact to connect you with support services and answer any questions you may have. She is a computer programmer with extensive project management and technical writing experience. She will track all project activities, ensure adherence to established deadlines, manage communications, and monitor each phase of your project from design to implementation.
- **Brent Leistner.** Mr. Leistner is your Server Room design Physical Security and Power Quality Team Leader. He has sixteen years' experience in the Information Technology (IT) field, from planning to development. Mr. Leistner will plan and implement physical security features to maximize productivity of your server room, including money- saving power quality management.
- **Christopher Mullenberg.** Mr. Mullenberg is your HVAC and Disaster Recovery Expert. He also has an extensive background in INTA and Digital Forensics, which adds to our network security profile. Mr. Mullenberg will ensure the proper cooling and ventilation of your server room, pre-install various security firewalls, and provide a feasible disaster recovery plan based on your staffing and controls.
- **Dung Phan.** Mr. Phan is your Server Room design Fire Prevention Team Leader. He has experience in Information Technology Network Administration and safety systems. Mr. Phan will develop a fire prevention system tailored to your unique space and controls.

Distribution of Work: The Report

Work for this project is highly collaborative, allowing each person to contribute their strengths and support other team members. Each report section has a *Section Leader* from the pool of team members. Each team member leads up to two report sections. The Project Manager manages the project, contributes to all sections as appropriate, and is responsible for writing the project summary, compiling the project plan and submission of the plan and final report.

Each team member is encouraged to contribute relevant ideas, content, and suggestions as discovered, to support the work of each Section Leader. The Section Leader creates original

content and evaluates related contributions from other team members. Section Leaders work with the Project Manager to develop section drafts including Section Leaders' original content and relevant ideas from team submissions.

The Project Manager collects section drafts, compiles, edits, and formats submissions, and requests or completes revisions as appropriate. The Project Manager also moderates the entire discussion forum to keep the project moving forward. Section Leaders are as follows:

- Physical Security (Brent Leistner)
- HVAC (Christopher Mullenberg)
- Fire Suppression (Dung Phan)
- Power Quality (Brent Leistner)
- Business Continuity (Shenica Graham)
- Disaster Recovery (Christopher Mullenberg / Dung Phan)
- Summary (Shenica Graham)

Shenica Graham will also take the lead to manage planning, discussions, revisions, formatting, final editing, and submission of the final project report.

Section Scope

Physical Security

The Section Leader will complete the *Physical Security Planning Worksheet* developed by IBM.

The scope of this section includes the following topics:

- Server security
- Server reliability (uptime)
- Public Access
- Staff Access
- File encryption
- Video surveillance
- Biometric access controls
- Automated site backup
- Firewall technology
- Redundant Tier 1 Internet connections

- N+1 redundant battery & diesel power
- Redundant HVAC and 24x7 on-site security & technical support.
- Failure mitigation
- After hours system maintenance
- Application upgrades with posted notices
- Automated alert systems

This section will answer the following questions:

- Where will you put the system unit?
- Where will you locate each display station?
- Where will you locate printers?
- What additional equipment do you need, such as wiring, telephone lines, furniture, or storage areas?
- What measures will you take to protect the system from emergencies such as fire or power interruptions?

HVAC (Heating, Ventilation, and Air Conditioning)

Continuous temperature and humidity control is vital to the proper functioning of the data system as the equipment dissipates substantial heat while in constant operation. The scope of this section includes the following topics:

- Air conditioning determination
- General guidelines for data centers
- Temperature and humidity design criteria
- Temperature and humidity recording instruments
- Relocation and temporary storage
- Acclimation
- System air distribution

This section will answer the following questions:

- What controls will you implement to ensure proper temperature and humidity regulation year-round?
- How much heat dissipation can be expected from the data center?

- How many personnel will be required to operate the system?
- What are the lighting requirements?
- How much fresh air can be introduced in the data center location?
- Will there be reheating of circulated air?
- Will there be heat conduction through outer walls and windows?
- What is the necessary ceiling height?
- What floor area is required?
- What is the number and placement of door openings?
- What is the number and height of partitions?

Fire Suppression

The scope of this section includes the following topics:

- Further plans should include training of personnel to act in an emergency. Sound alarm signals for fire detection and for other abnormal conditions to familiarize personnel with the alarm.
- Monitor the computer room, air conditioning equipment room, and electrical and data storage room at all times.
- Inspect steam pipes and water pipes above the false ceiling to guard against possible damage due to accidental breakage, leakage, or condensation.
- Locate emergency exit doors in the computer area. The number of doors depends on the size and location of the area. Train personnel in emergency measures such as:
 - Shutting off all electrical power
 - Shutting off the air conditioning system
 - Shutting off the chilled water to the information technology equipment
 - Calling the fire company
 - Handling fire extinguishers in the approved manner
 - Operating a small-diameter fire hose
 - Evacuating records
 - Evacuating personnel
 - Administering first aid

This section will answer the following questions:

- What are the possible types of fire and how do you extinguish each type?
- What are the most common fire suppression systems?
- Which fire suppression system(s) do you recommend and why?

Power Quality

Electrical power quality affects electronic equipment performance. The scope of this section includes the following topics:

- General power information
- Power quality
- Voltage and frequency limits
- Power load
- Power source
- Dual power installations
- Uninterruptible Power Source

This section will answer the following questions:

- What controls will you implement to ensure that quality power is available to the data system?
- What are the power requirements?
- What should be considered when evaluating emergency power supply options? For example, how does one choose between gas-powered generators versus a battery-powered emergency power supply?

Business Continuity

The scope of this section includes the following topics:

- Vibration and shock
- Lighting
- Acoustics
- Electromagnetic compatibility
- Computer room location

- Material and data storage protection
- Emergency planning for continuous operations

This section will answer the following questions:

- What information needs to be backed up and what backup strategies and plans need to be considered?
- Are backups stored onsite and offsite? If onsite, are the backups stored in fireproof safes? If offsite, how readily are the backups available in case of emergencies? Are backups tested regularly?
- Are technologies such as Microsoft Cluster Server in place?
- What Redundant Array of Inline Disks (RAID) system implementations are in place?
- Is there a record of critical systems hardware and software configurations?
- What training is required so operators and administrators can respond in a timely and professional manner?
- What records need to be maintained in order to recover from a failure or disaster?
- Is there an incident response team available to in case of emergency?
- Where are licensed software packages kept and what onsite support is there from vendors?
- Have fire drills been practiced by the incident response team and security officials?

Disaster Recovery

The scope of this section includes the following topics:

- Plans and procedures should already be developed before a failure occurs. Most the time, when a failure occurs and continuity of operations is halted for a prolonged period, it is because procedures and plans have not been developed correctly.
- The software configuration of systems should be maintained. This includes operating system versions, service pack updates, and any other software.
- You should keep track of hardware configurations such as disks and partitions; peripheral devices installed; and IRQ, DMA, and I/O addresses.
- Always ensure that backups are current and up to date. If possible, perform trial restore operations to test backups.

- Implement new technologies such as Microsoft Cluster Server. Microsoft cluster server technology will be discussed later in the paper.
- Implement RAID technologies. These are also discussed later in the paper.
- It is also possible in some cases to implement standby servers. Backed up information is restored on a computer that is purely for redundant purposes.

This section will answer the following questions:

- How many people should staff the disaster recovery site?
- Do staffing requirements differ in “hot site” and “cold site” environments?
- What types of procedures should a staff follow before and during a disaster?
- When should an outside staff be hired for a disaster recovery site?

Summary

The scope of this section includes the following topics:

- Pre-installation recommendations
- Post-installation recommendations
- Included services
- Nominal fee services

This section will answer the following question:

- Why should DMACC Enterprises choose Rock e Tech services over the competition?

Sources

- “Business Continuity and Resiliency Services.” <http://www-935.ibm.com/services/us/en/it-services/business-continuity-and-resiliency-services.html>
- “Criteria for Staffing a Disaster Recovery Site.” <http://searchdisasterrecovery.techtarget.com/feature/Criteria-for-staffing-a-disaster-recovery-site>
- “Emergency Planning for Continuous Operations.” http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/index.jsp?topic=%2Fiphad_p5%2Fcontinuousoperations.html
- “Evaluating Emergency Power Supply Options.” <http://searchdisasterrecovery.techtarget.com/answer/Evaluating-emergency-power-supply-options>
- “Fire suppression Systems and Your Data Center Disaster Recovery Plan.” <http://searchdisasterrecovery.techtarget.com/tip/Fire-suppression-systems-and-your-data-center-disaster-recovery-plan>
- “NIST Special Publication 800-12: Computer Security. An Introduction to Computer Security: The NIST Handbook.” <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- “Physical building properties to evaluate during server room design.” <http://searchdatacenter.techtarget.com/tip/Physical-building-properties-to-evaluate-during-server-room-design>
- “Physical Security Guidelines.” <http://www.dps.mo.gov/homelandsecurity/safeschools/documents/FBI%20-%20Physical%20Security%20Guidelines.pdf>
- “Planning Physical Security.” <http://publib.boulder.ibm.com/infocenter/series/v5r4/index.jsp?topic=%2Fzamu%2Fzamuplanphysec.htm>
- “Property Loss Prevention Data Sheets.” http://www.shuw.org/wp-content/uploads/FMDS1005_DisasterRecovery.pdf
- “Security Plan Document.” <http://www.docusourceofnc.com/files/8712/4579/2761/DocuSource%20Security%20Document%20V2-3%201008.pdf>
- “Security Planning.” Microsoft Technet. <http://technet.microsoft.com/en-us/library/cc723503.aspx>

“Server Room Planning.” <http://www.servervaulting.com/serverroomplanning.asp>

“Site Preparation and Physical Planning.”

<http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/topic/p7ebel/p7ebel.pdf>.

“Temperature and Humidity Design Criteria.”

http://pic.dhe.ibm.com/infocenter/powersys/v3r1m5/index.jsp?topic=%2Fiphad_p5%2Ftempandhumiditydesign.htm