

Best Practice Checklist Series - Issue 10

Equipment Storage, Security and Power Continuity

Understanding the basics: A layperson's guide and checklist for overseeing IT.

Best Practice Checklist Series

An exclusive publication of Sandbox Technologies, Inc.

3868 W Carson St, Suite 316
Torrance, CA 90503
Tel. (424) 207-5130
www.sandboxtech.com

SANDBOX TECHNOLOGIES

Small Business Solutions
Enterprise GrowthPath®
EGP Secure®
EGP Cloud™
ConstructIT®

Equipment Storage, Security and Power Continuity

Giving due consideration to the storage, security and power continuity of network equipment is sadly an area of IT that is often neglected until it's too late.

Failure to maintain networking equipment in a suitable environment that is both secure and meets the recommended cooling and power requirements can have serious ramifications. Similarly, unless due attention is given to power continuity, organizations run the risk of sustaining serious financial damages and lost productivity in the event a sustained loss of power should occur.

Because the consequences for every organization can vary, this area of focus demands that business owners and management be apprised of the various risks and select the appropriate protections for their organization based on their tolerance for risk.

For elaboration on any of the subject matter discussed herein, do not hesitate to contact your Sandbox Technologies Engineer, Account Manager, or Consulting CIO for additional assistance or information.

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Table of Contents

Equipment Storage 4
Equipment Security 7
Power Continuity 8

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Equipment Storage

Proper Storage

Are all devices stored within a stable enclosure that is seismically secured?

The ability for solid state electronics to sustain damage from falls and even slight jarring is highly unpredictable. On occasion, servers are known to have fallen as far as five feet onto hard surfaces without sustaining material damage, yet on other occasions, similar equipment has been known to suffer permanent data loss and failure of critical components as the result of being slid into rail kits too aggressively.

Best practices suggest that the most universally accepted means of storing servers and other key network equipment is to properly mount them inside a secure data cabinet that is seismically anchored to mitigate the likelihood of falls or impacts.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Hazard Avoidance

Are devices positioned safely away from water-based fire suppression systems (sprinkler heads), pipes that could potentially leak or burst, as well as other potential hazards, and is suitable fire suppression equipment in place?

Optimally, network equipment should be secured far from any building infrastructure that could cause damage in the event of activation or malfunction. Halon-based fire suppression systems that can be triggered to deplete oxygen in the event of a fire emergency are the recommended means of fire suppression for sensitive electronic equipment.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Static Prevention

Have suitable flooring materials and measures for discharging harmful static electricity been installed?

It has been our good fortune that Sandbox Technologies has yet to encounter an equipment failure that we can attribute to the absence of static dissipative flooring material. Notwithstanding this fact, there is little dispute over the fact that that sensitive electronic equipment can sustain damage as a result of static discharge, so in keeping with our commitment to best practices, the use of static dissipative flooring material is recommended when resources permit.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Climate Control

Does the environment where devices are maintained provide suitable air flow and fall within the recommended cooling and humidity standards?

Temperatures and recommended humidity ranges can vary slightly and are to some degree subject to the size of the room in which the climate is being controlled. Generally speaking, server room temperatures should range between 64-80°Fahrenheit or 18-27°Celsius. Humidity levels should range roughly between 40-60% rH. When selecting a suitable climate control system for an environment, there are numerous calculations that should be taken into consideration, including the current and projected maximum heat output of equipment in BTU's (British Thermal Units), the cubic footage of the room that is to be climate controlled, heat output from light fixtures and other equipment, and even the estimated BTU output of the maximum number of persons that will concurrently occupy the space. (Studies suggest that based on a 2,000-calorie diet, a human body generates roughly 330 BTU's of heat per hour.)

While the foregoing level of attention to heat and humidity considerations is rarely given to equipment rooms supporting small to medium-sized businesses, the process of projecting heat output and identifying the optimal cooling solution is actually relatively simple when the principles are understood. While the expense of engaging a professional infrastructure specialist may seem prohibitive, businesses are often pleasantly surprised when the specialist finds the (often arbitrary) cooling solution choices made by architect and space planners to be unnecessary overkill.

Perhaps more importantly, when equipment overheats, hardware damage can occur resulting in immediate failure, or (often worse) aberrant malfunctions that manifest intermittently and cause frustration, loss of productivity, and IT troubleshooting charges that have at times been known to climb to $10,000 or more before the problem occurs at the right time and is identified. Adding insult to injury, if an analysis by the original equipment manufacturer (OEM) determines that a problem was the result of overheating, most OEM's will void the hardware warranty and require the purchaser to reimburse any costs associated with remediating the resulting problems.

In short, many SMB's have been to operate without incident for decades with little or no climate control measures in place, however if it is believed that there is any reason for concern regarding the suitability of your current climate control, or if a new climate control solution is being planned, then obtaining professional advice is strongly recommended and the minimal investment can pale in contrast with the expenses that can result from the use of an inadequate system.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Power

Is equipment connected to one or more dedicated circuits meeting recommended load requirements?

Networking equipment should always be connected to dedicated electrical circuits that meet the minimum load specifications of the attached equipment. Failure to do so can result in overloads and potential damage to equipment. A qualified electrician should always be consulted to confirm power suitability. It should be understood that with rare exceptions, structured network cabling installers work with low voltages, and are not electricians. Only certified electricians should be relied upon to verify or validate specifications for conventional 120 Volt power implementations.

Status ☐ ☐ ☐

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Equipment Security

Enclosed, Locking Equipment Cabinet

Is networking equipment maintained in one or more four-post, enclosed, locking data cabinets?

It is by no means unusual for organizations to dismiss the possibility of theft or vandalism to their network equipment as being unlikely. While the decision to invest in enclosed data cabinets is one that must be made by those responsible for the physical security of company assets and data, it is perhaps worth noting that at the time of this writing, the cost of a data cabinet is roughly $2,000.00 plus installation.

It is recommended that the cost of such a cabinet be compared to the investment in the contents, and then consider that although rare, in over two decades in business, our organization can attest to the fact that numerous losses have been incurred as a result of break-ins and internal thefts targeted at clients opting to forego the use of enclosed, locking data cabinets.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

MDF Access Control

Is a solution in place for controlling access to the organization's main distribution frame "MDF", often also referred to as its' server room?

Similar to the previous recommendation, maintaining a locked MDF is essential to mitigate the likelihood of incurring equipment damage or a total loss due to theft or malicious acts. Employing a solution that electronically logs access and access attempts can aid investigative efforts in the event such should occur.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

Power Continuity

Uninterruptable Power Source (UPS) and Other Power Continuity Solutions

Does the organization have suitable measures in place to ensure suitable continuity in the event of various power loss scenarios, and do the applicable decision makers have an accurate understanding of the level of protections in place?

There are various degrees to which an organization may wish to employ power continuity solutions. Most SMB's opt for more cost-effective, yet less robust battery-based power backup solutions that provide power conditioning and backup power that typically provides uptime long enough to allow users to save data and for systems to be shut down gracefully.

Three phase power continuity systems provide power over longer periods of time, which can prove invaluable should the organization experience a long-term power outage. While such systems provide true continuity, they are often cost-prohibitive for small to medium-sized businesses. Additionally, the installation of three phase systems typically requires significant infrastructure and space, which can be difficult to negotiate in commercial rental locations, and particularly in hi-rise buildings where options are limited.

Smaller battery backup units typically only provide enough power to sustain functionality during momentary power outages, permitting equipment to be shut down gracefully via the use of agents installed and configured on protected devices. Although such systems provide negligible power continuity, they play an important role by mitigating the likelihood of data loss or corruption when outages occur.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

UPS Configuration

If a UPS battery backup unit is in place, is it properly configured to initiate the graceful shutdown of attached equipment?

Most business-class UPS appliances feature software and cables that are used to connect the UPS device to interfaces in the attached devices and trigger graceful shutdowns in the event that the UPS detects a power outage. Without proper configuration, when a power outage is prolonged to the extent that the UPS battery becomes depleted, attached devices will lose power and not be shut down gracefully as intended.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

© 2021, All Rights Reserved. Sandbox Technologies, Inc.

UPS Testing

If a UPS battery backup unit is in place, is tested periodically to confirm viability of the battery and its ability to provide the necessary continuity in the event of a power outage?

Like any other type of battery, UPS batteries have a limited shelf life and their ability to store and supply power diminishes over time. Most commercial UPS battery backup appliances include an alerting feature that causes the device produce an audible alert when the device determines that its battery is no longer viable.
Notwithstanding this feature, UPS battery backups should be tested periodically, and it is recommended that batteries be replaced in keeping with each battery's recommended lifecycle, regardless of alert status. (Note: Because UPS battery backups employ the use of solid-state hardware to provide the "intelligence" behind the battery, the actual hardware lifecycle is such that a depleted battery can typically be replaced once with a marginal chance of other hardware failure occurring.

It is not recommended that UPS batteries be replaced more than once, as the likelihood of a non-battery related failure becomes greater over time, such that the investment in a third replacement battery may be wasted if another component of the UPS unit should subsequently fail shortly thereafter.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

This document is protected by US and International copyright laws. Reproduction or distribution of this document for commercial advantage and without written permission from Sandbox Technologies, Inc. is strictly prohibited. Any distribution must retain attributions and this notice.

© 2021, All Rights Reserved. Sandbox Technologies, Inc.