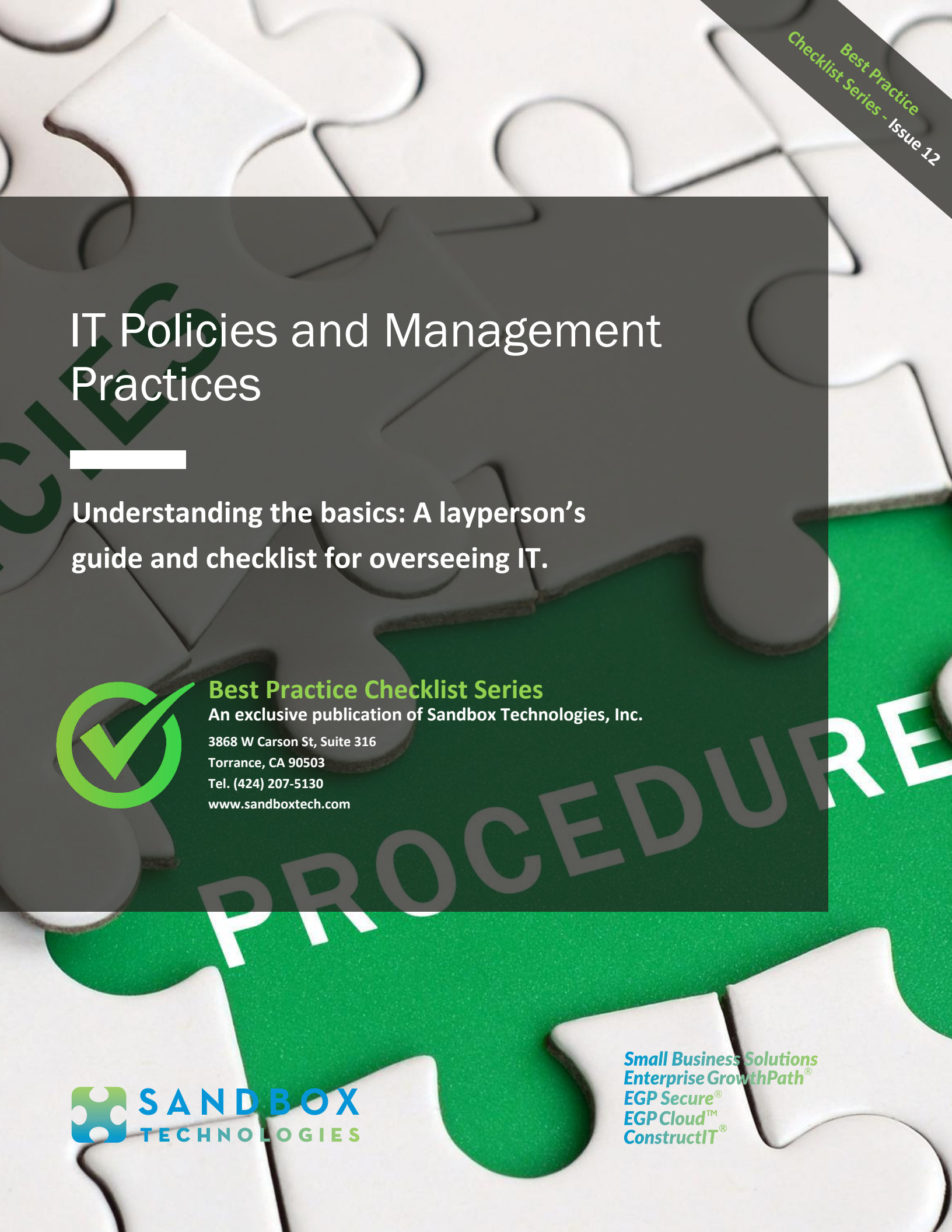


Best Practice Checklist Series - Issue 12

IT Policies and Management Practices

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®

IT Policies and Management Practices

Sound policies and management practices are the foundation of a successful information technology infrastructure. They not only play an essential role in ensuring smooth operations, they're also crucial to mitigating security risks and the exposure to liability that can result from a data breach.

If you would like assistance with the development of your organization's IT policies and management practices, Sandbox Technologies is here to help. For more information, contact your Sandbox Technologies Engineer, Account Manager, or Consulting CIO.

SANDBOX TECHNOLOGIES

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

Table of Contents

IT Policies and Management Practices 4

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

IT Policies and Management Practices

Documentation

Does the organization maintain formal documentation of the network, including network diagrams, equipment/rack elevations and detailed hardware/software asset inventories?

Documentation is key to effective IT management. For more information about network documentation, see Best Practice Checklist Series Issue #11, "Network Documentation".

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Asset Tagging and Tracking

Are company IT assets tagged and maintained in an asset tracking system?

Formal asset tracking helps to mitigate loss and aids in creating a planned obsolesce framework to ensure that systems are replaced within their recommended lifecycle (typically 3-4 years) before age and hardware degradation cause undue maintenance overhead and downtime.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

IT Budget/Forecasts

Does the company create and maintain annual budget forecasts?

IT budgets play an important role in ensuring that software and systems continue to meet the company's needs, that necessary hardware and software upgrades occur timely, and that contingency funds are allocated for incident response efforts when required.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Employee Onboarding & Termination Procedures

Are formal procedures in place for clearly communicating employee onboarding and termination requirements between HR and IT?

Formal onboarding and termination procedures guide IT regarding the creation and removal of users, and the assignment of equipment. In the absence of formal procedures, time is often spent clarifying instructions and/or remediating mistakes resulting from incomplete information. Improperly creating or removing users can also lead to exposure, particularly when users are assigned permissions they should not have, or when accounts and/or permissions are not properly removed.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Documenting Non-Standard Configurations (Power Users, Third-Party Service Accounts, etc.)

Does the organization maintain documentation of all non-standard configurations? (Power users, authorized administrators of third-party solutions, social media accounts, etc.)

The documentation of non-standard user configurations is key to avoiding the creation of security flaws when users are moved and/or replaced. Without complete knowledge of each user's rights and permissions in the environment, it is possible to inadvertently allow access that should be restricted or restrict access that is authorized.

Internally, documentation should include Active Directory rights and group inheritance, VPN access rights, as well as non-standard rights to internal systems like ERP solutions, accounting software and payroll processing interfaces. Access to external systems, ranging from third party mail hosts to social media accounts should likewise be tracked and documented.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

User Information Technology Policies

Does the organization maintain (and update, as necessary) formal policies governing the use of its information technology systems?

IT policies may vary by organization and are often subject to change with the introduction of new technologies and legislation. Inclusion of policies addressing the following topics is recommended, subject to prior review and approval by qualified legal counsel.

Recommended policy topics:

- Employee responsibilities regarding the safeguarding of passwords.
- Practices for the protection of confidential information.
- Maintaining physical security of equipment (laptops, smart phones, etc.)

SANDBOX TECHNOLOGIES

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

- Proper use of access to systems, responsibilities & limitations.
- Prohibitions against unauthorized technical changes & modifications.
- Restrictions prohibiting the unauthorized use of software, web solutions and equipment not provided by the company.
- Virus awareness & avoidance.
- Responsibility to attend company sponsored employee/contractor security training and awareness.
- External media handling and disposal.
- International travel security policies.
- VPN & mobile device use.
- Unlawful or unauthorized use of systems.
- Unauthorized removal, copying, deletion, and/or dissemination of information.
- Electronic use of company logo, & branding imagery.
- Blogging/Social media use policies & restrictions.
- Compliance with copyright law.
- Confidentiality policies & guidelines.
- Restrictions governing torrents & questionable websites.
- Inappropriate communications, harassment & discrimination.
- Company ownership of and rights to monitor/view/record all information transiting company's systems (in addition to conventional network resources, consider addressing third party hosting facilities, Cloud solutions, smart phones, and other connected devices as applicable.)
- Clearly state company policy concerning employee and contractor privacy expectations when using company systems.
- Post-termination employee/contractor conduct.
- Return or destruction of company electronic information.
- Duty to assist, provide passwords as needed.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

IT Department Security

Does the organization maintain formal policies governing the administration its Information Technology Department?

Given their role in administering systems, IT personnel often possess unrestricted access credentials. This inherent necessity creates a point of weakness that is particularly common in smaller enterprises. Engaging highly qualified individuals, conducting background checks, and performing periodic audits can reduce exposure. However, one of the most effective controls is the implementation of internal standards and the implementation of utilities that facilitate audit trails. Standards will vary according to each organization's needs, and may include topics such as data sanitization practices, software approval requirements, discrete administrative rights assignments, Active Directory controls, and equipment & media disposal.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Outside Vendor Security

Does the organization have a formal process for evaluating third party vendor security?

Before engaging an outside vendor, it is important to conduct a review of the vendor's security and that of any associated technologies they may employ in connection with the performance of their job functions. A vendor security questionnaire requests relevant data points to aid in assessing whether or not the vendor's security meets an organization's standards.

Examples of data requested may include security audit results, development practices, system redundancies, support options, response times, upgrade schedules, maintenance windows, backup and retention policies/schedules, change management processes, and access requirements.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Audited Vendors

When available, are third party vendor audit results reviewed?

Many vendors fall under compliance regulations (PCI DSS, FINRA, etc.), and must undergo periodic audits to verify both security and compliance. It is important to be familiar with each vendor's security practices and processes. Vendors entrusted with sensitive information, and/or those permitted to connect to customer systems should be familiar with their organization's compliance measures. Some vendors publish their compliance information online, and those that do not will generally provide it to customers upon request.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Data Security

Does the organization have a system established for classifying data sensitivity?

Effectively managing data security requires that it be identified effectively. Examples of sensitive data include access credentials, HR, and related information (social security numbers, bank account numbers for direct deposit, etc.), sensitive client data, company trade secrets, financial data, creative content, and internal forecasts.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Change Management

Are formal procedures in place to facilitate change management?

Change management is beneficial for ensuring that proposed changes to an environment or workflow processes do not create new vulnerabilities, conflict with existing configurations, or cause unintended consequences on business operations.

.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Information Security Plan

Does the organization have a formal information security plan?

An Information Security Plan or Information Security Program (ISP) identifies risks to an organization's security, lists safeguards employed, and details the various measures to be followed as part of a formal IT security program. It identifies individuals responsible for overseeing data security, and addresses topics such as employee management and training, procedures for documenting and securing areas where sensitive data is stored, secure data destruction, detecting and managing system failures, and protocols for periodically evaluating and adjusting the ISP.

Many organizations may be unaware of legal obligations that require them to maintain an Information Security Plan. As an example, the GLBA Safeguards Rule, which applies to organizations involved with the preparation of tax returns, calls for an information security plan that meets requirements outlined by the IRS.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

Backup and Disaster Recovery Plan

Does the organization have a formal backup and disaster recovery plan?

A written Backup and Disaster Recovery (BDR) plan outlines the steps, order of action and team member responsibilities in the event of a disaster. A properly implemented DR plan facilitates a rapid and more seamless response in the event of a loss or failure, with the objective of minimizing both data and productivity losses due to downtime.

Status ☐ ✓ ☐ – ☐ ?

NOTES: _____

_____

_____

SANDBOX TECHNOLOGIES

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

Incident Response Plan

Does the organization have a formal incident response plan for managing cybersecurity incidents?

No environment is one hundred percent secure. The increased occurrence of social engineering attacks has been so dramatic many experts say that for most business, breaches are much less a matter of “if” than “when”.

A written Incident Response Plan outlines the steps, order of action and responsibilities assigned to individuals, allowing the response to a cybersecurity event to be quicker and more seamless. An effective response can help to reduce downtime, data reconstruction requirements, forensic expenses, mandatory notification costs, legal fees, publicity fees, reputation damage and loss of revenue, by rapidly curtailing exposure.

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.