Best Practice Checklist Series - Issue 5

Authentication Security, Network Traffic & Activity Analysis

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®

Table of Contents

Authentication Security & Activity Analysis....3
When it goes wrong....4
- The reused password....4
- The second factor that was not there....4
- The breach no one could see....4
- The shared administrator login....4
- The common thread....4

What to Ask Your IT Manager or Provider....5
- Passwords Built for Strength, Not Forced Complexity....5
- No Reused or Shared Passwords....5
- Phishing-Resistant Multifactor Authentication....6
- Separate, Unique Administrative Accounts....6
- A Master List of Credentials Held by Management....6
- A Proper Password Repository....7
- Third-Party Vendor Access on Request....7
- Automatic Screen Locking....7

Seeing What Happens on the Network....7
- Traffic Analysis or a SIEM With Alerting....8
- Centralized, Durable Audit Logging....8
- Web Use Monitoring, Where Appropriate....8
- Physical Access Control and Visitor Logging....9

Terminology....9
- Why the multifactor method matters....9
- The shift in password thinking....9
- Web use monitoring: the legal considerations....9

© 2026 Sandbox Technologies, Inc.

Authentication Security & Activity Analysis

Most intrusions do not pick the lock. They sign in.

Almost every serious intrusion now begins the same quiet way: with a valid username and password, used by the wrong person. The defenses that matter here are not exotic. They decide how an identity is proven, how administrative privilege is separated, and whether anyone can later see what happened. When those choices are weak, an attacker does not break in. They log in, and often no one notices until long after.

© 2026 Sandbox Technologies, Inc.

When it goes wrong

No set of controls makes an account impossible to misuse, and chasing that is not the goal. The aim is narrower: to make a stolen credential hard to use, and its misuse easy to see. The situations below are ordinary, not exotic, and they occur more often than most organizations realize.

The reused password

An employee uses one familiar password for a personal shopping account and, for convenience, the company VPN. Months later the shopping site is breached and that password appears on a list traded among attackers. Automated tools then replay it against business logins.

The second factor that was not there

Multifactor authentication is switched on for the main sign-in page. An older mail protocol, left enabled for a legacy application, still accepts a password on its own. An attacker holding a phished password connects through that path and is never prompted for a code.

The breach no one could see

An intruder is present for months. Device logs are sparse and clear themselves on reboot, and nothing gathers them in one place. When the activity is finally noticed, there is no record of what was reached or taken.

The shared administrator login

Several IT staff, and one departed contractor, all knew the same administrator password. A change is made that should not have been, or data leaves. The audit log shows only “administrator.”

The common thread

None of these turns on a firewall or an exotic exploit. Each was decided in advance by three things: how an identity was proven, whether one credential could be traced to one person, and whether the activity left a trail anyone could read.

Every one of these outcomes could very likely have been avoided. Not with a larger security budget, but with a few deliberate choices about how people prove who they are, how administrative privilege is separated, and whether activity is recorded. That is the whole of this issue.

© 2026 Sandbox Technologies, Inc.

What to Ask Your IT Manager or Provider

and how to know if the answers are good ones

You do not need to administer an identity platform or a monitoring system to oversee one. You need to know what to ask. A short primer on the finer points is provided at the end, for those who want the detail. First, the part that matters: run the checklist below with your IT professional. If any item is not marked green, it may warrant a closer look.

Passwords Built for Strength, Not Forced Complexity

Are password rules based on length rather than forced complexity, and are new passwords screened against lists of known-breached passwords? Current guidance from NIST (Special Publication 800-63B) favors longer passphrases, a minimum in the range of 12 to 15 characters, over the older pattern of mandatory upper case, lower case, number, and symbol rules, which tended to produce predictable substitutions such as “@” for “a.” The same guidance no longer recommends forcing scheduled password changes on a fixed calendar; passwords should be changed when there is reason to believe they have been compromised. Screening new passwords against known-breached lists does more for security than complexity rules ever did.

Compliant	NOTES:
Needs Attention	
N/A	

No Reused or Shared Passwords

Are unique passwords used for every system and service, and never shared between people? Attackers know that one password often unlocks many doors. After breaching a single site or service, they routinely replay the same credentials against everything else, a technique known as credential stuffing. The exposure is greatest for administrative credentials and core network devices, where one reused password can cascade across the environment and amplify the damage.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Phishing-Resistant Multifactor Authentication

Is multifactor authentication required for all company resources, and are the stronger, phishing-resistant methods used where they are supported? Multifactor authentication (also called 2FA) adds a second proof beyond the password and remains one of the most effective controls available. Not all methods are equal: one-time codes sent by text message or generated by an app can be phished or intercepted, while phishing-resistant methods based on the FIDO2 standard, including passkeys and hardware security keys, are designed to resist those attacks. It is equally important to close older protocols that can still accept a password on its own and quietly bypass the second factor.

Compliant	NOTES:
Needs Attention	
N/A	

Separate, Unique Administrative Accounts

Does each administrator have a unique administrative login, kept separate from their everyday user account? Shared administrative credentials make disclosure more likely and forensic investigation far harder, because the logs cannot distinguish one person's actions from another's. They also add labor when an administrator leaves, since every shared account and dependent service, task, and automation must be changed. Keeping administrative accounts separate from day-to-day accounts also limits the damage if a routine account, used for email and browsing, is compromised.

Compliant	NOTES:
Needs Attention	
N/A	

A Master List of Credentials Held by Management

Does a designated, trusted, non-technical member of management maintain a secure and comprehensive list of administrative credentials to company systems? This practice helps prevent systems from being held hostage by a disgruntled employee or vendor, and avoids an awkward scramble for passwords during a personnel change or an inspection. Other executives of equivalent rank or higher should know who holds this responsibility.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

A Proper Password Repository

Are passwords kept only in a purpose-built, secured password manager, and never in email, instant messages, spreadsheets, or ordinary documents? Password protection on everyday documents is weak and can often be bypassed. A suitable repository should require its own multifactor authentication and, ideally, keep an audit trail of who accessed which credential and when. Organizations that adopt a well-regarded cloud-based manager should understand that doing so places considerable trust in that provider, since such systems are high-value targets; some organizations prefer to host their own behind a multifactor-protected VPN.

Compliant	NOTES:
Needs Attention	
N/A	

Third-Party Vendor Access on Request

Is remote access by third-party vendors limited to those who genuinely need it, and granted per use where access is only occasional? Vendors sometimes need access to provide maintenance, support, and upgrades, but every party with access widens exposure. For vendors who need only occasional access, it is reasonable to require a written request and to enable access on a manual, per-use basis rather than leaving a standing door open.

Compliant	NOTES:
Needs Attention	
N/A	

Automatic Screen Locking

Are workstations set to lock automatically after a short period of inactivity, and are users reminded to lock their screens whenever they step away? An unattended, unlocked workstation is an open door to anyone with physical access. A centralized policy, locking after no more than about fifteen minutes and sooner where practical, is easier to verify and maintain than settings left to each individual machine.

Compliant	NOTES:
Needs Attention	
N/A	

Seeing What Happens on the Network

detection, logging, and the record you will wish you had

Strong authentication decides who gets in. This second group decides whether anyone can see what happens next, in time to act and, later, to prove. The same rule applies: if an item is not green, it is worth a closer look.

© 2026 Sandbox Technologies, Inc.

Traffic Analysis or a SIEM With Alerting

Does the organization use a traffic analysis or SIEM solution that flags unusual or potentially malicious activity for someone to review? A SIEM (Security Information and Event Management) tool gathers activity from across the network and surfaces anomalies: the outbound connections that malware and botnets often create, unusually large offsite data transfers that can signal theft, or non-secure connections to unsanctioned services. As one example, repeated outbound attempts to addresses in countries where the company does no business may merit a look. At a minimum, it is worth having an automated solution that reviews activity, escalates likely threats for human review, and retains logs long enough to be useful after the fact.

Compliant	NOTES:
Needs Attention	
N/A	

Centralized, Durable Audit Logging

Are auditing utilities in place that aggregate logs from across the environment and retain them beyond a device reboot? Built-in logging is often minimal and can vanish when a device restarts. Third-party audit tools bridge that gap by preserving a durable, searchable record. It serves several purposes: establishing who did what when an administrative action is disputed, surfacing misconfigurations worth correcting, and, after a breach, helping identify what was actually reached. A good audit trail can be the difference between notifying every customer out of caution and notifying only the few whose records were genuinely touched.

Compliant	NOTES:
Needs Attention	
N/A	

Web Use Monitoring, Where Appropriate

If the organization monitors or limits web use, has it been introduced thoughtfully and with legal guidance? Web use monitoring can protect proprietary data and productivity, but it carries cultural and legal considerations and is not right for every environment. Where it is used, policy should make clear that users have no expectation of privacy on company systems, and certain roles may warrant additional care. The finer points, including steps that reduce liability, are covered in the primer below, and legal counsel should confirm what is appropriate for the organization.

Compliant	NOTES:
Needs Attention	
N/A	

© 2026 Sandbox Technologies, Inc.

Physical Access Control and Visitor Logging

Are there suitable measures to restrict physical access to authorized people and to log visitors in and out? Electronic sign-in systems, cameras, and visitor badges deter opportunistic theft and raise awareness of who is on the premises, and they matter most where sensitive data is housed or high-value equipment is stored. The value varies by organization; smaller offices should weigh the real likelihood of unauthorized access against the cost before investing.

Compliant	NOTES:
Needs Attention	
N/A	

Terminology

Why the multifactor method matters

Not every second factor resists a determined attacker. Codes sent by text message can be exposed through SIM-swap fraud, and both texted and app-generated codes can be captured by a convincing fake login page that relays them in real time. Repeated approval prompts can also wear a user down until one is accepted by mistake. Methods built on the FIDO2 standard, including passkeys and hardware security keys, are bound to the genuine site and are designed to resist these attacks, which is why they are described as phishing-resistant. Where a platform does not yet support them, an authenticator app is generally preferable to text-message codes.

The shift in password thinking

Guidance has moved away from short, complex passwords changed on a fixed schedule. Current NIST guidance (SP 800-63B) emphasizes length over enforced complexity, screening new passwords against lists of known-breached ones, and allowing long passphrases. It also advises against forcing routine password changes on a calendar, since that practice tended to produce weaker, predictable variations; a change is warranted when there is evidence a password may have been compromised. Organizations subject to specific compliance requirements should still follow the rules that apply to them.

Web use monitoring: the legal considerations

Where web use monitoring is deployed, a few precautions reduce liability. Personnel whose roles require visiting destinations that might otherwise be considered inappropriate can be exempted from filtering, and it is often recommended that such work be done through virtual browsing sessions to reduce the risk of malware. For roles likely to surface objectionable material, organizations sometimes obtain written legal acknowledgements, adjust position descriptions, add privacy screens, or position displays to limit what others can see. In every case, the organization should seek the guidance of its legal counsel to determine what is suitable.

© 2026 Sandbox Technologies, Inc.

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.

© 2026 Sandbox Technologies, Inc.