BEST PRACTICES FOR

SUPPORTING APPLE TECHNOLOGY IN BUSINESS

A starting place for SMB & Mac/iOS footprints in large & enterprise organizations

SPRINGBOARD IT

Premier Partner

INTRODUCTION

Whether you're a start-up or a well-established company, your success hinges on the performance of your technology. This means having a strategy in place to protect, support, and secure your assets, users, and data.

Macs are so easy to use. However, that may put people in a false sense of security around the IT plan for Apple devices. **Many businesses are missing critical IT best practices.**

With over 20 years of experience supporting Apple technology, our engineers and technicians have developed Best Practices for Supporting Mac in Business. As Apple IT experts, we strongly emphasize formulating a strategy to put these best practices into action.

? DO YOU HAVE AN IT STRATEGY?

LIKE GOOD FINANCIAL PLANNING AND ADMINISTRATION, IT PLANNING AND ADMINISTRATION IS CRITICAL TO HEALTHY AND SCALABLE GROWTH.

BEST PRACTICE ✓

It may sound obvious, but so many small-medium businesses don't start with a strategic and holistic vision for IT strategy. They are letting business needs dictate quick decisions around technology and leaving major gaps around items like support and security.

Once you're in a healthy growth state, a lack of IT strategy will become a growing heap of "technical debt." Not having a strategy will create disconnected systems, redundant costs in software solutions, and higher security risks.

You may not have someone on staff to handle these concerns directly, but someone on the leadership team should be in charge of addressing a strategy and plan for your IT.

Building an IT plan is important and this guide is a practical start to get you thinking about different IT components. There's many additional considerations to build on after this guide, but with this start, you'll be well on your way to building a scalable plan.

WHAT'S MISSING FROM YOUR IT PLAN?

ARE YOU MISSING ANY OF THESE KEY AREAS? IF SO, THIS GUIDE CAN HELP YOU UNDERSTAND SOME BEST PRACTICES TO START YOUR IT STRATEGY

Most of these relate to two areas of concern in a business: productivity and security. Having these two ideas addressed strategically in the below core areas will help you build a strong business.

1. Enterprise grade networks
2. Company owned devices are centrally managed
3. Leverage cloud collaboration/productivity platforms
4. Data backed up continuously and redundantly
5. Endpoint protection/security scanning continuously
6. Modern, accessible file sharing solutions
7. Hardware that is updated regularly
8. Top rated line of business applications
9. Strategic IT leaders or partners

1 ENTERPRISE GRADE NETWORKS

COMMON PRACTICE

Consumer grade or low end business class networks with limited security and traffic shaping features

BEST PRACTICE ✓

BUILD AN ENTERPRISE-GRADE, CLOUD MANAGED NETWORK INFRASTRUCTURE

You may not know it, but creating a stable and secure network is complex. The price point and features that some consumer and low grade business network equipment boasts can be enticing, but it will cost you more money with the amount of time you lose to an inconsistent network.

Enterprise grade solutions that are cloud managed will allow you to see and troubleshoot your network quickly. If an outage happens you can track it easily to remedy it. You can secure your team against dangerous websites. The bandwidth is more intelligently allocated on the network ensuring people can reliably connect and stay connected.

2 DEVICE MANAGEMENT

COMMON PRACTICE

Macs/iOS devices are not managed; there is no way to remotely secure, lock or update; Apple Business Manager is not setup for the organization

BEST PRACTICE ✓

APPLE SPECIFIC MDM THAT ALLOWS REMOTE, CENTRALIZED MANAGEMENT

Many companies don't believe the risks don't outweigh the cost to implement a device management solution or they trust their team to stick to company policy.

But, what would you really do if one of the company's Macs was lost or stolen? What do you do if a remote employee needs to be off-boarded, but has their device? You need to be able to remotely lock devices, enforce passwords upon login, updates to software and more in order to keep them secure.

With growing remote workforces and security needs, implementing a solution for remote management is critical to the data security of an organization.

3 COLLABORATION IN THE CLOUD

COMMON PRACTICE

Not on MS 365 or G Suite backbone; email files back and forth for changes/collaboration; no internal chat tools

BEST PRACTICE

✓

IMPLEMENT INDUSTRY LEADING CLOUD COLLABORATION & COMMUNICATION TOOLS

Today’s modern business requires flexibility, adaptability, and mobility when it comes to shared assets.

Implementing a secure, cloud-based team collaboration strategy ensures emails, calendars, contacts and other shared resources can be managed and shared with users inside and outside of your organization. It can also help prevent overwriting mistakes and encourages collaboration. Additionally, these modern cloud collaboration tools usually work with other leading SaaS applications which will assist in your team's overall productivity.

4 CONTINUOUS & REDUNDANT BACKUPS

COMMON PRACTICE

Macs not backing up to anything; G Suite/Microsoft instances not backed up; only one back up

BEST PRACTICE ✓

PUT CONTINUOUS AND REDUNDANT BACKUPS IN PLACE FOR CRITICAL ASSETS

Keeping your data safe and secure is more important than ever. An automated backup strategy that includes both on and offsite backups, as well as monitoring of backup health and connectivity, minimizes data loss and downtime in the event of system failure or ransomware attack.

If your users ever work off the desktop, having the ability to restore files in the case of emergency will be worth the backup costs. If you have servers, file shares, and other business critical tools like email or a CRM, make sure you are taking a regular backup that is secured separately from your live assets.

5 ENDPOINT PROTECTION

COMMON PRACTICE

Has no anti-virus/endpoint protections running on Macs; uses home/free version of AV; thinks Macs don't need anti-virus; no spam filters for email

BEST PRACTICE ✓

INSTALL VIRUS & MALWARE (ENDPOINT) PROTECTION ON EVERY ENDPOINT

Despite common belief, Macs are not immune to malware. Ransomware, spyware and other harmful attacks left undetected can have major consequences for a business. Users may not recognize suspect links or files. Remote workers without secure DNS are even more at risk without the extra layer of protection the firewall gives.

We insist that every Mac endpoint and server is equipped with best in class virus and malware protection to keep you safe from all kinds of threats without slowing you down. We also encourage you to do Security Awareness Training regularly for your users to help prevent phishing leaks and downloading malware.

6 MODERN FILE SHARING

COMMON PRACTICE

Mac users are forced to work with traditional server tools; large files are not locally optimized; servers are not secured by permissions; Mac mini server still in use

BEST PRACTICE ✓

UTILIZE A MODERN AND APPLE FRIENDLY FILE SHARING SOLUTION

Life happens, If there is a power outage or disaster strikes and your company is running on an old or unsecured server, everything you've built your business on could be at risk.

We recommend an up to date and modern file sharing solution complete with local and offsite backup, be proactively monitored to ensure health and connectivity. NAS solutions are often platform agnostic and work with other backup and cloud collaboration tools.

We also encourage teams to set up permissions on their servers to prevent unwanted access to sensitive company data.

7 HARDWARE LIFECYCLES

COMMON PRACTICE

Run equipment until it dies; don't have a refresh cycle; have machines that are no longer able to run supported operating system/software

BEST PRACTICE ✓

OPERATE ON A HARDWARE LIFECYCLE WITH MODERN, CAPABLE HARDWARE

Maintaining a healthy refresh cycle for your Mac hardware ensures you are always getting the most out of your technology budget.

Springboard IT supports Macs that are newer than 5 years old and running recent versions of Mac OS to guarantee your business operates at peak performance at all times. We offer attractive leasing options as well as trade-in programs for old equipment to make it easy to stay up to date.

8 TOP-RATED LINE OF BUSINESS SOFTWARE

COMMON PRACTICE

Use software that doesn't get regular updates or out of date versions; software is not standardized across the organization; current software developer doesn't have roadmap that meets business needs

BEST PRACTICE ✓

USE TRUSTED SOFTWARE SOLUTIONS THAT GET REGULAR UPDATES

With so many software providers to choose from, selecting the right option for your business can be overwhelming and time-consuming. More importantly, if you choose the wrong software for your business, you could be pouring thousands of dollars down the drain.

If you are on legacy software, the longer you stay on it, the more painful and expensive it is to migrate away. We recommend using recent, currently supported versions of popular software solutions to ensure compatibility with other business partners and organizations.

9 STRATEGIC IT TEAM OR PARTNER

COMMON PRACTICE

IT "firefighting;" IT handled by owner, office admin or developer; IT solutions implemented ad-hoc as needed; Apple IT plan not considered important

BEST PRACTICE ✓

GET IT LEADERS OR PARTNERS THAT HELP YOU TAKE A STRATEGIC APPROACH

The glue that holds any IT strategy in place, is a trust-worthy, dependable, and professional strategic partner. Business goals should be aligned with the IT team's priorities. Even if your Apple footprint is small, it could be a significant gap in your plan (especially considering many times executives request to work on Macs). Owners handling IT is a waste of money and office admins can only get so far.

You may be trying to sign a big client and not be prepared when they ask about your firewall or access management. You may not have a plan when ransomware gets on your server. These are all avoidable by planning or partnering with an outside consultant who can help make this plan with your stakeholders based on your industry, business goals, budget and more.

STILL PUZZLED? WE CAN HELP!

You don't have do it all on your own. Whether you have no IT team or just need some Apple expertise, we offer monthly IT services at a flat monthly fee or flat fee projects to assist your business in each of these areas. If you've never looked at outsourced IT help, start with us!

CONTACT US
CALL: (215) 988-7770
EMAIL: INFO@SPRINGBOARDIT.COM
VISIT: WWW.SPRINGBOARDIT.COM

Premier Partner