ZAG
Technical Services

Cisco Partner

Advanced Security Architecture Specialization
Networking Specialization
Premier Integrator
Select Provider
Registered Partner

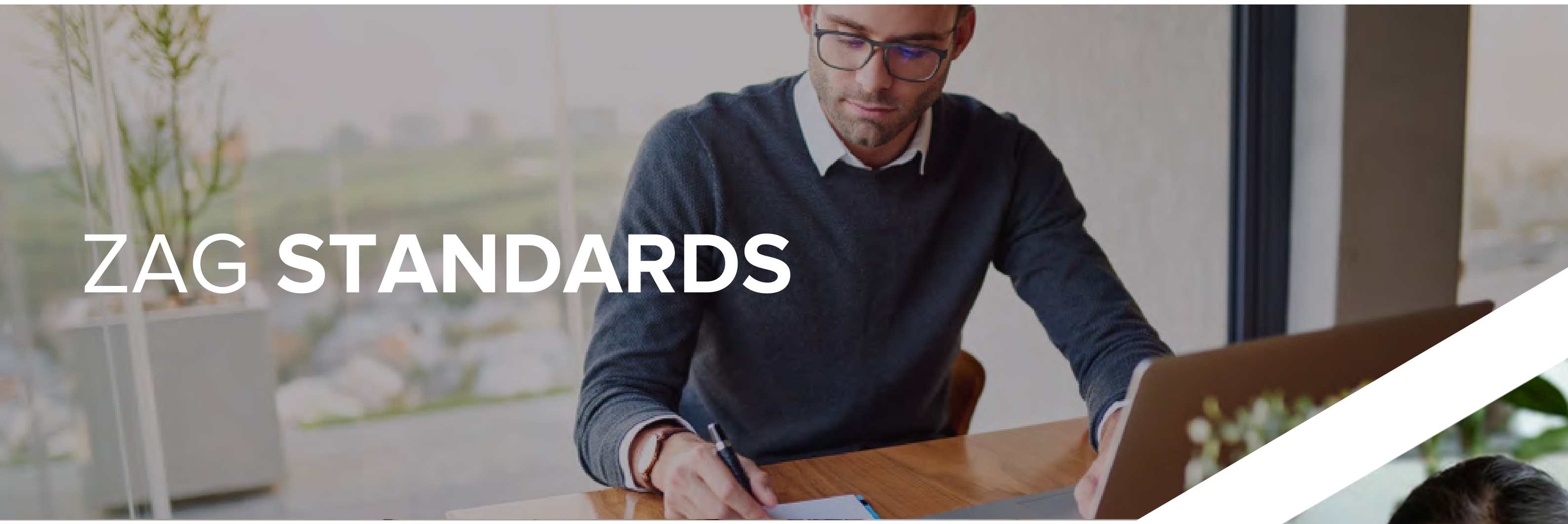
IT Security Best Practices for Manufacturing

Actionable security standards for your email, workstations, and network, plus disaster recovery and IT asset management best practices.

Based on more than 200+ standards and 22 years serving America's critical infrastructure businesses.

INCLUDES FREE CYBERSECURITY INCIDENT RESPONSE CHECKLIST

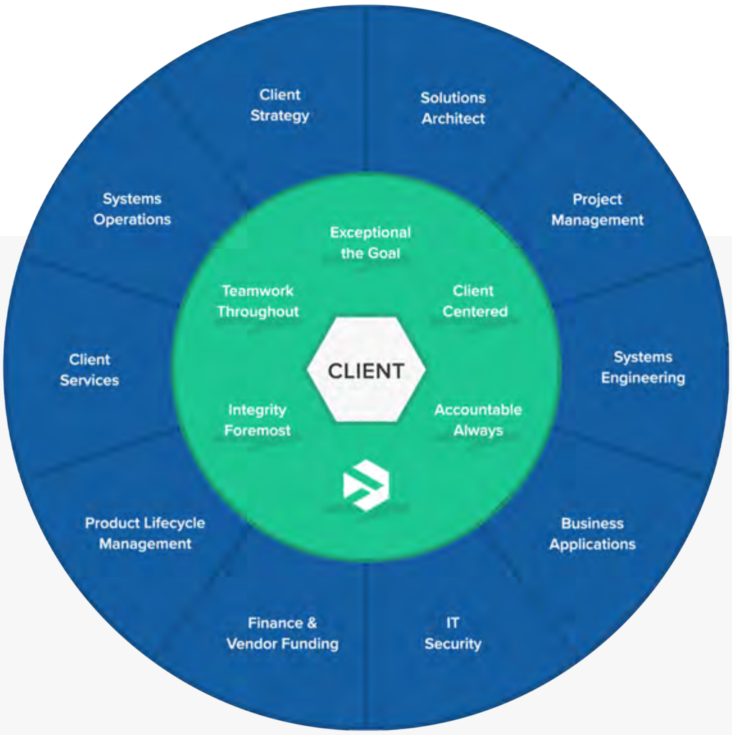
ZAG
Technical Services



ZAG **STANDARDS**

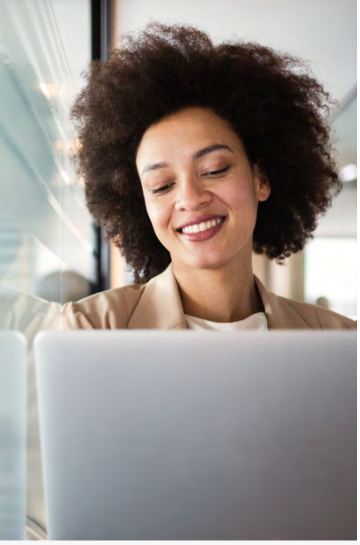
200+ **STANDARDS**

When it comes to your business, one of the best things you can do is find a managed service provider that takes industry standards seriously. Implementing best practices within your IT environment – from your workstations to management strategies and everything in between – is going to give you the best chance for success. Over time, ZAG has compiled over 200 technology standards and best practices that are used as tools to assess the environments of our clients, ensuring that their IT environment is as optimized as possible.



CLIENT **CENTERED**

ZAG takes a client-focused approach with every project and engagement. We surround the client with our strategy, commitment to excellence and the resources they need to succeed.



ACTIVE DIRECTORY

Without the proper standards in place, Active Directory can be a breeding ground for security concerns that can ultimately cause data breaches, harmful malware infiltrations, accidental changes and more. Here are a few of the top standards used by ZAG on Active Directory environments:

- Rename local admin accounts so that they are not set to vendor defaults.
- Use of discretion when adding users to groups with high levels of access (i.e., domain admin and local admin for example).
- Use of tiered access to separate everyday users from those that need administrative functionality.

DISASTER RECOVERY

A solid disaster recovery solution with well-defined test plans is something every business should have in their continuity plan. Without it, you're opening yourself up to data loss and downtime, two things no business leader wants to think about. These standards should be put into place to protect your business from unforeseen outages due to anything from equipment failure to ISP circuit issues:

- Document your disaster recovery architecture and failover plans.
- Thorough User Acceptance Testing documentation that outlines what applications are deemed critical in a failover situation and how they should function.
- Keep updated digital and hard copies of all disaster recovery diagrams and test plans in case of emergencies.
- Simulated failover testing on a quarterly basis.

EMAIL

Email is one of the most heavily used tools in the business world. These standards help keep communications secure, preventing hackers from accessing personal data like user credentials, accounting information, credit card numbers and more.

- Mandatory use of Multi-factor Authentication (MFA) on all user and service accounts.
- Data Loss Prevention (DLP) policies that alert users when emails are received from outside the company, when forwarding rules are set up, and when other critical events occur.
- Policies that outline where accounts can be logged in from, prohibiting international hackers from accessing email inboxes in well-known hacking regions.

IT ASSET MANAGEMENT

Standards for managing assets and technical strategy help improve business development and align with your company's budget, saving you time and money. Here are a few of ZAG's many management standards.

- Design of a clear roadmap that defines how your business will evolve its IT infrastructure.
- Keep accurate and updated records of all customer assets, including licenses and hardware.

NETWORK SECURITY

Network security should be a top concern for every company, and utilizing these best practices will keep your environment protected from harmful attacks.

- Keep firmware levels on all physical equipment up to date, allowing for functionality and feature enhancements, as well as protection from security threats.
- Replace standalone and disparate networks at branch locations wherever possible to create one cohesive network architecture.

SERVERS

Servers are where much of a business's critical information is stored and accessed. These standards should be put into place to protect your data from being breached or lost due to an unforeseen outage or equipment failure.

- Keep OS up to date.
- Conduct regular backups of all production and failover servers.

WIRELESS

Wireless networks can be a huge pain point for businesses from a security standpoint. These standards not only help protect business data from outsiders, they also help optimize your network so your employees can get the most out of it.

- Configure policies that prohibit unauthorized devices from accessing the internal network.
- Design wireless access point maps based on specific business needs, including placement and configuration.

WORKSTATION

Workstations are the most heavily used pieces of equipment in any business, and ensuring that proper industry best practices are put in place for managing these devices is critical. These standards help protect your business at the most basic level.

- Conduct regular patching of all workstations to ensure they receive up to date security and feature enhancements.
- Keep accurate records of all workstation OS levels through detailed asset management.
- Take regular backups of workstations to prevent data loss due to hardware malfunctions.

ZAG Technical Services

CISCO Partner

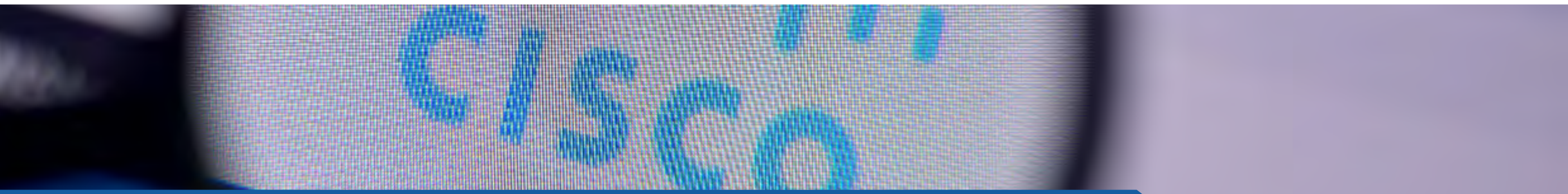
Advanced Security Architecture Specialization
Networking Specialization
Premier Integrator
Select Provider
Registered Partner

Cyber Incident Response Checklist

26 best practices and action items to help your business recover from a serious cybersecurity incident.

- ❑ Disable RDS password storage
- ❑ Disable AD Domain cached credentials
- ❑ Disable LLMNR & NetBIOS Over TCP/IP
- ❑ Remove Local Administrator “debug” rights
- ❑ Disable browser-based password storage
- ❑ Disable Service Account Interactive login
- ❑ Deploy Tiered Administrative Accounts
- ❑ Enable Windows Firewall
- ❑ Disable SMBv1
- ❑ Monitor changes to sensitive groups
- ❑ Action “PrintNightmare” Remediation
- ❑ Enable MFA for all remote access methods
- ❑ Enable MFA for all administrative server logins
- ❑ Enable MFA for all end-user workstation logins
- ❑ Enable MFA for SaaS applications
- ❑ Enable MFA for vCenter logins
- ❑ Apply modern password policies
- ❑ Isolate backup systems
- ❑ Enable immutability for backup storage
- ❑ Private cloud architecture for Hyper-V
- ❑ LAPS for Local Administrator Password Control
- ❑ Enable SAN-based snapshots for critical servers
- ❑ Deploy a password manager with MFA for all users
- ❑ Deploy BitLocker to all workstations
- ❑ Deploy Sysmon to all endpoints
- ❑ Block unneeded geographies from SaaS logins

Not sure where to start? Contact our team of experts for a complimentary cybersecurity consultation.



ZAG Technical Services | www.zagtech.com | info@zagtech.com | 408.383.2000

CISCO Partner

ZAG Technical Services