

CYBERSECURITY CHECKLIST

White Paper

*A Practical Guide
to Securing
Firms in a High-
Risk Digital
Landscape*

EXECUTIVE SUMMARY

Cyber threats are becoming increasingly sophisticated and frequent, putting organizations of all sizes and types at risk. With sensitive data, intellectual property, and critical operations on the line, businesses cannot afford weaknesses in their digital infrastructure. In many environments, decentralized teams and a wide range of stakeholders can make consistent cybersecurity practices difficult to implement.

This checklist provides IT leaders, project managers, and executives with essential security best practices. Use it as a baseline to assess your current cybersecurity posture and as a roadmap for reducing risk and ensuring compliance readiness..

Call us at: **714-777-3222** or send us an email at: **info@ironorbit.com**

Follow for More!



SECURITY CHECK LIST

Multifactor Authentication (MFA):

- ☐ Enforce MFA across all remote access, cloud platforms, and email systems.
- ☐ Require MFA for accessing project data and critical applications (e.g., BIM tools).

Access and Availability

- ☐ Use high-security facilities with redundant environmental controls.
- ☐ Using bio-metrics and other control methods to restrict access to key systems and data.
- ☐ Use surveillance methods to monitor activities.

User Access Management

- ☐ Properly screen, onboard, and train users on proper system use.
- ☐ Unique user access for all users.
- ☐ Implement role-based access controls (RBAC).
- ☐ Enforce least privilege principles across shared drives and project portals.
- ☐ Review access rights quarterly and deactivate dormant accounts.

Patch Management

- ☐ Apply OS and application security patches depending on urgency, but at least monthly.
- ☐ Use automated patching tools to remediate a majority of vulnerabilities and focus on key items.
- ☐ Maintain a vulnerability management log.
- ☐ Prioritize CVSS Scores and tie urgency to real-world exploitability.

Endpoint Protection

- ☐ Deploy EDR\XDR (Endpoint\Extended Detection and Response) on all company devices (both local and virtual).
- ☐ Deploy (Subscribe) to real-time service to monitor suspicious behavior and anomalous activity.
- ☐ Use device control policies to enforce encryption and limit USB/external drive usage.

Secure Configuration Baselines

- ☐ Harden configurations of all servers, workstations, and firewalls.
- ☐ Disable unnecessary ports, protocols, and services by default.
- ☐ Benchmark against industry standards (e.g., CIS Benchmarks).

Web Application Security

- ☐ Perform regular scanning for OWASP Top 10 vulnerabilities (e.g., SQL injection, XSS).
- ☐ Deploy Web Application Firewalls (WAFs) to protect against real-time threats.
- ☐ Enforce HTTPS on all external sites using valid SSL/TLS certificates.

Incident Response Plan

- ☐ Maintain a written incident response plan with playbooks, escalation paths, and defined communication protocols.
- ☐ Conduct annual tabletop exercises to simulate real scenarios.
- ☐ Integrate SIEM tools to automate detection, tracking, and documentation of incidents.

Data Encryption

- ☐ Encrypt data in transit (SSL/TLS), stored, and at rest (AES-256 standard).
- ☐ Use full disk encryption on all external data sources, laptops, and field devices.

Backup and Recovery

- ☐ Maintain daily backups with 30-day retention.
- ☐ Test backup restoration quarterly.
- ☐ Store backups in isolated, immutable locations.

Email Security and Phishing Protection

- ☐ Enable advanced threat protection. Maintain user security awareness training at onboarding, annually, and regular re-enforcements (ie phishing simulations and education)
- ☐ Enable sandboxing for email attachments.

Vendor Risk Management

- ☐ Assess third-party vendors for security compliance.
- ☐ Require SOC 2 Type 2 reports or a signed security questionnaire from all key vendors.
- ☐ Maintain a vendor security checklist and audit log.

Compliance and Documentation

- ☐ Maintain a complete Information Security Policy with supporting policies for incident response, data handling, change management, etc.
- ☐ Ensure compliance with SOC 2, CMMC, or ISO 27001 depending on client requirements.
- ☐ Update policies as changes occur, review annually, and communicate them to the staff.

Call us at: **714-777-3222** or send us an email at: **info@ironorbit.com**

Follow for More!



CONCLUSION & NEXT STEPS

Cybersecurity is not a one-time initiative, it's an ongoing practice. While this checklist provides a strong foundation, threats are constantly evolving. Regularly reassess your tools, processes, and employee behaviors to stay ahead.

For maximum effectiveness, complement this checklist with routine audits, third-party penetration testing, and a strategic security roadmap aligned with your organization's risk profile and long-term objectives.

NEED HELP EVALUATING YOUR CURRENT CYBERSECURITY MATURITY?

IronOrbit's vCISO (Virtual Chief Information Security Officer) services deliver tailored strategic security leadership for organizations seeking expert guidance without the cost of a full-time executive. Our security professionals assess your current posture, assist in policy development, oversee compliance efforts, and support the implementation of key controls outlined in this checklist.

From risk assessments and incident response planning to vendor management and ongoing employee training, our vCISO offering brings the value of an experienced security leader aligned to your business goals and risk profile.

WHY IRONORBIT?

The client chose IronOrbit for its track record of delivering secure, highly redundant cloud solutions. With a deep commitment to business continuity and 24/7 proactive monitoring and US-based support, IronOrbit provides them with peace of mind, and a technology foundation built for the future.



IronOrbit is Recognized in the 2023 and 2024 Gartner Magic Quadrant for DaaS (Desktop as a Service) and is included in the 2021 & 2023 Gartner Market Guide for DaaS.

Call us at: **714-777-3222** or send us an email at: **info@ironorbit.com**

Follow for More!

