# RYMARK'S Security Audit Guide

## SAFEGUARD YOUR ORGANIZATION FROM CYBER THREATS

### PROTECTION

**Technology Discovery & Risk Profile Assessment**

RYMARK performs a network assessment to develop a practical profile of the customer environment. This process helps identify visible risks, aging infrastructure and areas that should be prioritized in improving the environment's overall security posture.

**Patching & Critical Update Management**

Critical patch management, software updates, and next-gen real-time antivirus protection to help safeguard your IT assets and network(s) against the latest cyber threats and security vulnerabilities

**Network Security**

Enforce & proactively manage Intrusion Prevention, Gateway Antivirus, DNS Protection, Web Blocker, spam blocker, Geofence VPN, Secure Wi-Fi & application control to provide greater security for your internal network.

- ☐ Firewall/Model: _____
- ☐ DNS Protection

**Email Security**

Advanced spam filtering & phishing protection includes: anti-spam, anti-virus, ransomware defense, zero-day virus protection, spear-phishing, CEO fraud protection, & dedicated IP recovery from blacklisting.

- ☐ Email filtering ☐ Email Encryption
- ☐ DMARC/DKIM policy

**Password & MFA Management**

Restricted accounts and privileges. Password policy documentation and policy enforcement.

- ☐ M365/Google MFA ☐ Local MFA
- ☐ Password Manager

**IT Asset Management**

System and software auditing. Inventory and tracking, Asset lifecycle management, cost optimization, increased compliance and security.

**Data Backup**

Backup management to protect your mission-critical data and minimize downtime in the event of a failure or cyberattack.

- ☐ Local backup ☐ Cloud backup
- ☐ M365/Google Cloud backup

**Privileged Access Management**

RYMARK's PrivilegeShield secures administrative access by enforcing least privilege, controlling elevated permissions, and reducing unnecessary user privileges across supported systems.

**Security Awareness Training**

Empower employees with ongoing security awareness training, phishing simulations, and compliance reporting to reduce risk and strengthen your organization's security posture.

**Identity Security Posture Management**

Continuously assesses and strengthens identity security by identifying risky configurations, excessive privileges, weak authentication controls, stale accounts, and configuration drift across supported cloud environments.

**Mobile Device Management**

Secure and manage mobile devices with centralized policies, remote configuration, monitoring, and device management to protect corporate data and support compliance.

**Device Encryption Management**

HIPAA, FINRA ALTA or other compliance regulations? Lost or stolen devices? Encryption is the most effective way to achieve data security. It renders data unreadable if it falls into a criminal's hands.

### DETECTION

**Identity Threat Detection & Response**

Continuously monitor user identities and detect suspicious activity across Microsoft Entra ID and Google Workspace to identify account compromise, credential threats, and unauthorized access.

**Managed Endpoint Detection & Response**

Proactive Threat Detection: Detect and stop exploits and attacks nearly in real-time. Includes Security Operation Center monitoring, and remediation to prevent threat spread; predicts malicious behavior, quickly eliminates threats, and adapts defenses.

**Dark Web Monitoring**

Knowing in real time whether passwords & accounts have been posted for sale on the Dark Web allows you to be proactive in preventing a data breach. We scan the Dark Web & take action to protect your organization from stolen credentials.

**Client Business Review (CBR)**

A recurring strategic meeting to review IT performance, discuss emerging security threats, evaluate technologies that improve business efficiency, plan IT asset lifecycles, and ensure your technology strategy supports your business objectives.

**Security Information & Event Management (SIEM)**

SIEM provides continuous security monitoring and analysis across your environment by centralizing logs and events, detecting and investigating threats, and turning security data into actionable insights.

**Virtual Penetration Testing**

Proactively identify and remediate exploitable vulnerabilities before they impact your business.

Support compliance with PCI, HIPAA, SOC 2 and other regulatory standards.

### RESPONSE

**Help Desk Support**

Responsive IT support for your users, including trouble-shooting, technical assistance, and issue resolution to keep your team productive and your technology running smoothly.

**Security Operations Center (SOC):**

Around-the-clock security monitoring and incident response powered by experienced analysts, advanced threat detection, and rapid response to protect your organization and mitigate potential threats as quickly as possible.

**Disaster Recovery**

A valuable investment for any organization that relies on IT systems & data for its daily operations, IT DR is the process of restoring critical IT systems & data after a major disruption, such as a natural disaster, cyberattack or human error.

**Incident Response & Policy Procedures**

Documented company information security policies and response plans give employees guidelines to not only protect the organization from a cyberattack, but also provide clear direction in the event of a cybersecurity incident.

**Vulnerability Scanning**

Continuously identifies and prioritizes known vulnerabilities, missing updates, exposed services, and other security weaknesses across supported devices, networks, applications, and internet-facing assets.

**Cyber Insurance**

Cyber insurance can't protect your organization from cybercrime, but it can keep your organization on stable financial footing should a significant security event occur.

Client Name _____ Date _____

(651) 328.8900 | info@rymarkIT.com | rymarkIT.com