

# Microsoft 365 Security Best Practices for Resilience



## Strengthening Microsoft 365 Security for Cyber Resilience

As organizations modernize workflows and adopt cloud-based solutions, cybersecurity must remain a top priority. Microsoft 365 offers a robust suite of built-in security features designed to protect sensitive information, prevent cyber threats, and ensure compliance.

However, to fully leverage these capabilities, organizations must implement best practices tailored to their unique needs. This checklist is designed to help your organization anticipate, withstand, respond to, and recover from cyber threats using Microsoft 365.

### ANTICIPATE

**Enable Multi-Factor Authentication (MFA):** Protect user accounts by requiring at least two forms of authentication. Use authenticator apps like Microsoft Authenticator for added security over SMS-based MFA.

**Conduct a Security Assessment:** Regularly evaluate your Microsoft 365 environment to identify vulnerabilities and areas for improvement. Consider scheduling a professional Microsoft 365 Security Assessment.

**Understand Your Threat Landscape:** Stay informed about the latest cyber threats targeting your industry. Use Microsoft Defender's threat intelligence to anticipate potential risks.

**Develop Conditional Access Policies:** Set up policies to restrict access based on user location, device compliance, or risk level. For example, block logins from unfamiliar locations or non-compliant devices.

### WITHSTAND

**Deploy Microsoft Defender for Office 365:** Protect against phishing, malware, and ransomware by configuring Safe Links and Safe Attachments policies. Customize alerts to respond quickly to suspicious emails.

**Implement Role-Based Access Control (RBAC):** Limit access to sensitive data and systems by assigning roles with specific permissions. Regularly audit user permissions to ensure they align with current responsibilities.

**Utilize Data Loss Prevention (DLP) Policies:** Prevent accidental data breaches by creating DLP policies to monitor and block sharing of sensitive information, such as personal identifiable information (PII) or financial data.

**Adopt Zero Trust Principles:** Assume no user or device is automatically trusted. Use Microsoft 365's identity verification and least-privilege access features to enforce this model.

### RESPOND

**Monitor and Audit Security Logs:** Use Microsoft 365's logging capabilities to track system activities and detect unusual behavior. Leverage Microsoft Sentinel for advanced threat detection and response.

**Train Employees on Security Awareness:** Conduct regular training sessions to educate staff on identifying phishing, creating strong passwords, and reporting suspicious activity. Build a culture of security awareness to reduce human error.

**Develop an Incident Response Plan:** Create a clear plan for responding to cyber incidents, including steps for containment, communication, and recovery. Test the plan regularly to ensure its effectiveness.

### RECOVER

**Back Up Your Data:** Implement third-party backup solutions to protect against accidental deletion or ransomware attacks. Maintain at least two copies of your data – one in Microsoft 365 and another in a separate cloud backup.

**Ensure Regular Updates:** Keep all devices, software, and third-party integrations up to date. Use Microsoft Intune to enforce patching policies across your organization.

**Test Disaster Recovery Plans:** Simulate recovery scenarios to identify gaps and improve your ability to restore operations quickly after an incident.

### Ready to take the next step?

Visit [rehmann.com](https://rehmann.com) to schedule your Microsoft 365 Security Assessment today and ensure your organization is prepared to anticipate, withstand, respond to, and recover from attacks.