CLOUDGUARD
Security Done Different

ACTIONABLE SECURITY CONFIGURATION CHECKLIST

Businesses must continuously improve their cybersecurity posture, regardless of their investment level. Identifying and addressing exploitable gaps between different security products is crucial.

Recent Cybersecurity Events

Leicester City Council	RingGo	BRITISH LIBRARY	Ministry of Defence
NHS Dumfries & Galloway	NHS Guy's and St Thomas' NHS Foundation Trust	A&O	Microsoft

Even large organisations with significant investments face sophisticated cyber threats.

Regular Maintenance Tasks

□ **Weekly**

- □ Review and tune email security solutions.
- □ Check for new Azure privileged rights or left user accounts.

□ **Monthly**

- □ Audit and update certificates as needed.
- □ Review and resolve any new conflicting ENTRA conditional access policies.
- □ Monitor significant file extensions or movements for anomalies.

□ **Quarterly**

- □ Test Incident Response plans (2 areas)
- □ Audit and enforce strong password policies.

□ **Annually**

- □ Comprehensive review of all security policies and configurations.
- □ Update and retrain staff on security best practices and Incident Response protocols.

About CloudGuard

Cybersecurity isn't just a concern for giants in the industry. It's a necessity for businesses of all sizes.

That's why we created CloudGuard. We want to bring enterprise-level protection within reach of small to medium-sized businesses.

CloudGuard offers a Managed Security Service ecosystem that combines the latest technology with UK-based experts to protect your organisation 24/7. This allows you to focus on what matters - **growing your business**.

CLOUDGUARD
Security Done Different

□ Certificate Management

- □ Avoid using wildcard certificates for key public-facing services.
- □ Verify all public-facing services and protocols have correct, non-expired certificates.

□ Email Security

- □ Set active DMARC and DKIM policies
- □ Regularly tune email security solutions.
- □ Implement enhanced analytical rules to detect and prevent malicious content.

□ User Account Management

- □ Regularly audit and remove unused Azure privileged rights or left user accounts.
- □ Implement strict policies for account creation and deletion to avoid unnecessary privileged accounts.

□ Microsoft ENTRA Policies

- □ Review and resolve any conflicting ENTRA conditional access policies.

□ File monitoring

- □ Implement monitoring for significant file extension changes or unusual file movement.

□ Incident Response

- □ Ensure Incident Response plans are updated and tested regularly. Pick 2 to test every 3 months.

□ Password Management

- □ Avoid using known weak passwords for any account.
- □ Do not use password storage in browser applications.

□ Application Registration

- □ Restrict App registration capabilities to authorised users only.
- □ Regularly review App registration permissions and adjust as necessary.

□ Multi-Factor Authentication (MFA)

- □ Avoid over-reliance on MFA as the sole method of security.
- □ Regularly review and update MFA policies to close any gaps.
- □ Ensure MFA policies are comprehensive and applied to all users and groups.

□ Vulnerability Management

- □ Ensure all systems are regularly patched to address known vulnerabilities.

Have security concerns? We're here to help! → Contact Us