ClarioIT

ClarioIT Comprehensive Security Checklist
Last Updated: 2025
Strengthen your IT environment with this all-in-one security guide. Contact ClarioIT for a free assessment.

Identity and Access Management

- Enable Multi-Factor Authentication (MFA) for all users and admins.
- Implement role-based access control (RBAC) across systems.
- Regularly review and revoke unused accounts.

IT Infrastructure

- Ensure server hardware is updated with latest firmware.
- Implement network segmentation to isolate critical systems.
- Conduct regular backups with offsite storage (3-2-1 rule).

Cloud Solutions

- Enable Azure AD Conditional Access with location-based rules.
- Regularly patch cloud services (e.g., Azure, AWS) and monitor logs.
- Use encryption for data at rest and in transit.

Cybersecurity

- Deploy Microsoft Defender for Endpoint with real-time alerts.
- Set up a SIEM tool for centralized log analysis.
- Perform annual penetration testing to identify vulnerabilities.

Managed Services

- Enroll in 24/7 monitoring and incident response services.
- Schedule quarterly security health checks with your provider.
- Ensure SLA compliance for downtime and response times.

Artificial Intelligence

- Secure AI model training data with encryption and access controls.
- Monitor AI systems for anomalous behavior or data leaks.
- Train staff on AI-specific security risks (e.g., prompt injection).

Microsoft 365 Security

- Harden tenant settings: Disable legacy authentication.
- Activate Microsoft Defender for Office 365 with anti-phishing.
- Configure SharePoint/OneDrive DLP and external sharing limits.

Device and Endpoint Security

- Enroll devices in Intune with encryption enforced.
- Deploy security baselines via Intune/Autopilot.
- Enable Microsoft Defender for Endpoint with real-time alerts.

Email and Communication Security

- Configure DMARC, SPF, and DKIM for email domains.
- Block unverified senders and enable spam filtering.
- Train employees on phishing recognition quarterly.

Data Protection and Compliance

- Apply data classification and encryption standards.
- Set up backups with 3-2-1 rule (3 copies, 2 media, 1 offsite).
- Conduct annual compliance audits (e.g., GDPR, HIPAA).

Monitoring and Response

- Use SIEM tools for centralized log analysis.
- Test incident response plans biannually.
- Update security patches within 48 hours of release.

Employee Awareness and Training

- Conduct monthly security awareness sessions.
- Simulate phishing attacks to test vigilance.
- Document and enforce a clear security policy.

Regular Review and Improvement

- Check CIS Secure Score monthly (target +30 lift).
- Perform penetration testing annually.
- Adapt to new threats with vendor updates.

Download this checklist and schedule a free 30-minute consultation with ClarioIT to safeguard your organization.

Contact Us Today