IT SECURITY BEST PRACTICES CHECKLIST

Education and Awareness

- ☐ Host regular employee cybersecurity awareness education and training
- ☐ Periodically conduct blind phishing tests with varying complexity
- ☐ Assess at-risk employees and provide remediation training that targets their specific security weaknesses

User Access / Network and Remote Access

- ☐ Use Multi-Factor Authentication (MFA) for network access
- ☐ Use Multi-Factor Authentication (MFA) for remote access
- ☐ Have a password policy in place that meets password length/complexity requirements
- ☐ Restrict access to passwords and accounts based on who needs access and for how long
- ☐ Have access to logging for sensitive resources and systems administration
- ☐ Have a group policy set to lock workstations after 10 minutes of inactivity
- ☐ Have administrative and account access controls in place to ensure protection against insider threats
- ☐ Allow only company-owned and managed devices to access the corporate network
- ☐ Minimize mobile users' needs to access your organization's network infrastructure
- ☐ Enable mobile users to perform most of their work with Software as a Service (SaaS) tools[1]
- ☐ Allow secure[2] remote access to the company network only for specific roles and from company devices
- ☐ Implement content filtering
- ☐ Implement Geo-IP blocking on the firewall if the site has servers or a VPN published to the Internet[3]
- ☐ Disable USB ports for external drive use or implement USB encrypted portable storage devices

Wi-Fi Networks and Internet Filtering

- ☐ Use an internal company network Wi-Fi connection and only allow company-owned devices to connect
- ☐ Use a company Wi-Fi guest network for all non-company-owned devices (employee personal & guest)
- ☐ Utilize Internet perimeter protection including content filtering to block malicious or inappropriate web traffic
- ☐ Block the "uncategorized" category of websites to further minimize risk

Device OS and Encryption

- ☐ Encrypt all devices including laptops, desktops, and mobile devices
- ☐ Password-protect all devices
- ☐ Ensure all devices are running supported OS and current firmware

IT SECURITY BEST PRACTICES CHECKLIST

Mobile Device Management (MDM)

- ☐ Implement a Mobile Device Management (MDM) solution[4]

Email

- ☐ Use company email addresses only for company business
- ☐ Use multi-factor authentication for email access
- ☐ Implement third-party spam, virus quarantine service
- ☐ Use cloud-based commercial-grade email hosting
- ☐ Implement a Sender Policy Framework (SPF) record to check email sending host
- ☐ Implement Domain Keys Identified Mail (DKIM) to authenticate email source
- ☐ Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to fully utilize SPF and DKIM and act on false emails

Antivirus/Intrusion Detection

- ☐ Implement next-generation endpoint protection solution[5]
- ☐ Utilize intrusion detection software on all systems

Security Operations and Governance

- ☐ Have Computer and Internet Use Policy in place
- ☐ Proactively manage computer and software security updates, utilizing patch automation and reporting tools
- ☐ Consider a Security Information & Event Management (SIEM) system to consolidate computer security logs and help your security team review and investigate events
- ☐ Implement Security Operations Center (SOC) as a Service to analyze and act on SIEM-generated alerts
- ☐ Scan all machines for Personally Identifiable Information (PII)
- ☐ Subscribe to dark web scans looking for organization credential compromises
- ☐ Purchase cybersecurity Insurance

Disaster Recovery

- ☐ Establish and exercise a Business Continuity Plan
- ☐ Establish and exercise a Cybersecurity Incident Response Plan
- ☐ Repeatedly test the performance of the above plans and refine their policies and protocols as needed

Back Up

- ☐ Identify your organization's information assets and critical transaction tools[6]
- ☐ Identify recovery options that permit your organization to "undo" events and resume normal operations[7]
- ☐ Add to your SaaS providers' recovery offerings with 3rd-party solutions for higher confidence and flexibility[8]
- ☐ Account for your recovery option's Recovery Time Objective (RTO)[9] and Recovery Point Objective (RPO)[10]
- ☐ Ensure that your recovery option meets your organization's RTO and RPO needs[11]

IT SECURITY BEST PRACTICES CHECKLIST

Footnotes

1. Users should be able to access SaaS applications using just an Internet connection and their secure organization identity.
2. Secure the remote access connection via authenticated HTTPS tunneling (such as via Windows Virtual Desktop) or Virtual Private Networking (VPN) plus Remote Desktop Protocol (RDP).
3. Geo-IP blocking on a firewall is only relevant if the site has servers or a VPN published to the Internet; best practice is the corporate network should not have servers publishing to the Internet.
4. The MDM solution should, at minimum, provide the administrator with the capability to enforce a passcode, lock, and remotely erase the device or business information residing on the device.
5. Utilize a cloud-managed whitelist of known safe applications that can run on an endpoint.
6. Identify tools that are critical for daily, weekly, monthly, quarterly, and yearly operations.
7. Identify recovery options for each critical asset and business tool that enable your organization to restore system operating states or business information to points in time prior to damage, corruption, or loss.
8. Many SaaS providers include a basic level of recovery with their service, but many other SaaS providers exclude your organization's specific data from their recovery plans.
9. Recovery Time Objective (RTO); the time required to complete a recovery option and resume operations.
10. Recovery Point Objective (RPO); how frequently recovery points are established, and how long they are retained.
11. An economic target for most organizations of 25 to 75 people is a 6-hour RPO and 24-hour RTO for critical transaction/processing solutions, a 24-hour RPO and 48-hour RTO for e-mail or online file service solutions, and a 7-day RPO and 14-day RTO for archived and seldom-referenced content.