Password and Authentication Management

Promote Strong Password Hygiene
Require strong, unique passwords and encourage the use of password managers to securely store them.

Implement Multi-Factor Authentication (MFA)
Require MFA for accessing sensitive systems and data to add an extra layer of protection.

Utilize Passwordless Authentication
Encourage secure alternatives such as biometric authentication for sensitive applications.

Encryption and Secure Communications

End-to-End Encryption
Enforce encryption for all communications, including emails, messaging, and VoIP services.

Encrypt Data at Rest and in Transit
Ensure sensitive data is always encrypted, whether stored locally or transmitted over networks.

Network Security

Secure Wi-Fi and Network Traffic
Use WPA3 or VPNs to secure connections and deploy firewalls and intrusion detection systems to monitor traffic.

Segment Networks
Isolate IoT and less-secure devices from the core network to limit exposure in case of a breach.

Device and Account Security

Enforce Device Security Policies
Implement mandatory device locking, remote-wipe capabilities, and full-disk encryption on all company-issued devices.

Regular Software Updates
Ensure timely updates to all devices, apps, and firmware to mitigate vulnerabilities.

Mobile Device Management (MDM)
Use MDM solutions to enforce security policies, remotely wipe devices, and manage app usage.

Data Privacy and Minimization

Limit Data Collection and Retention
Collect only necessary data and securely delete it when no longer needed.

Provide Privacy Controls
Allow users to opt out of data collection and provide clear, transparent privacy policies regarding data handling.

Email Scanning Disclosure
Organizations should periodically notify their users of their email scanning policy.

Security Awareness and Training

Conduct Regular Training
Offer security awareness training on topics like phishing, social engineering, secure device handling, and safe online practices.

Simulated Security Drills
Regularly conduct phishing simulations and other security exercises to test employee readiness.

Secure Cloud and Backup Solutions

Encrypted Cloud Backup
Ensure cloud backups are encrypted and regularly audited for compliance with security standards.

Control Cloud Access
Implement strict permissions and two-factor authentication for cloud services to safeguard sensitive data.

Incident Response and Auditing

Develop an Incident Response Plan
Create a clear response plan for handling data breaches, including roles, communication protocols, and recovery steps.

Conduct Regular Audits
Perform routine audits of security practices, data handling, and third-party vendor compliance.

Physical and Environmental Security

Secure Devices Physically

Encourage the use of cable locks and secure storage options for devices, particularly during travel or remote work.

Monitor and Control Physical Access

Use secure printing and access controls for sensitive areas to prevent unauthorized data exposure.