October 2024

Supplier Security Guidance

Contents

Introduction

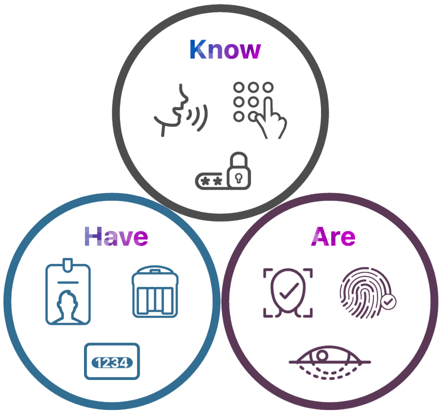
This guidance is intended to highlight some of the key security areas that Apple suppliers are expected to implement. While impactful, these measures alone may not be enough to ensure that your environment is secure, and some of these measures may not be appropriate in your particular context. It is essential that you work with security experts in your organization when designing your security program, and that you do not rely solely on this guidance.

Please also note that the guidance here is not intended to reduce any contractual obligations you have to Apple, including in any security addendum, such as the Information Security and Data Privacy Requirements. Review those requirements carefully to ensure that you comply with them. Apple recommends that you consult with your own counsel and experts to ensure that your organization is acting in compliance with local and national law.

Multi-factor Authentication

Multi-factor Authentication for Apple Suppliers

Authentication is the process or action of verifying the identity of a user or process to ensure a user is who they say they are before granting access to enterprise systems and applications. The most common form of authentication is the username and password combination. However, most hacking-related breaches involve guessing weak passwords or using lost or stolen credentials. Implementing multi-factor authentication (MFA) is a strong method to prevent these type of attacks. There are three types of authentication factors. MFA entails the use of at least two of the following three authentication
factors:



1: Something you know.

- username and password combination (Note: disable automatic login capabilities)
- Personal Identification Number (PIN)

2: Something you have.

- text message. A code sent via SMS to a mobile device as a second factor. (Note: Text messages could be unencrypted and are susceptible to hijacking and phishing attacks.)
- third-party authenticator application on a trusted device[1]. A downloaded authenticator application, stored on a user's trusted device, that generates a one-time code required after the user enters their credentials.
- hardware token. A small physical key, either inserted directly into a user's device, or connected via Bluetooth or another form of near-field communication (NFC), to log in.

3: Something you are.

The use of automated recognition of an individual by means of unique physical characteristics, such as:

- fingerprint reader (for example, Touch ID)
- facial recognition (for example, Face ID)
- Retinal Scan (for example, Optic ID)

[1] A trusted device is a device (for example, computer, phone, etc.) that is frequently used and that the user has designated that they own. The trust is derived from the assumption that the device should always be in the user's possession.

Multi-factor Authentication Guidance for Apple Suppliers

How do I enable MFA?

Many commonly used tools and applications already support MFA, organized under security settings or account settings. MFA might be listed as "Multi-factor Authentication," "Two-factor Authentication," or "Two-step Authentication."

Where IT services are outsourced to a third party, Apple recommends working with them to identify which tools, apps, and services support MFA, and enabling it where possible.

Where do I enable MFA?

Apple requires suppliers utilize MFA to access their environment infrastructure including, but not limited to:

- corporate virtual private networks (VPN)
- single sign-on (SSO) or identity access management (IAM) services
- email/webmail & calendar
- collaboration tools
- cloud-based services
- all internet-facing systems
- accounts and tools with privileged access (for example, administrative accounts, firewalls, routers, etc.)
- any system that can access, process, transmit, or store Apple data

For stronger protection, MFA should be enabled on all accounts
and devices that support the functionality. MFA is especially important for administrative users with access privileges beyond that of a standard user. For employees with access to the most sensitive or important data and systems, stronger authentication factors should be used where possible, including security keys and phishing-resistant MFA.

Phishing-resistant MFA

As security measures improve over time, cyber threat actors find ways to bypass MFA or gain access to a user's MFA credentials. Examples of these methods include phishing, SIM swap, and MFA fatigue. Accordingly, it's important to stay informed about developments in MFA technology.

The current gold standard in MFA is known as phishing-resistant MFA, which relies on recently
implemented standards including FIDO/WebAuthn authentication or public key infrastructure (PKI)-based authentication. Apple, along with Microsoft and Google, has recently begun supporting these new standards.

Passkey solutions have phishing-resistant benefits when compared to other MFA factors. Passkeys offer a user-friendly alternative to traditional passwords. They are a more secure, easier to use authentication method that work across most of a user's devices. Unlike passwords, passkeys are always strong and phishing-resistant.

Apple strongly recommends moving high-risk and critical systems to phishing-resistant MFA solutions where possible. Refer to the index for helpful articles for implementing MFA.

Industry Best Practices Related to Multi-factor Authentication

The table below references articles and benchmarks containing industry best practice guidance related to multi-factor authentication.

Industry Best Practices Related to Multi-factor Authentication	
Reference	Description
Apple	Two-factor Authentication for Apple ID: https://support.apple.com/en-us/HT204915 Passkeys: https://developer.apple.com/passkeys/ https://www.nist.gov/blogs/cybersecurity-insights/giving-nist-digital-identity-guidelines-boost-supplement-incorporating About Security Keys For Apple ID: https://support.apple.com/en-us/HT213154
Google	Enforce uniform MFA to company-owned resources: https://cloud.google.com/identity/solutions/enforce-mfa Passwordless Login with Passkeys: https://developers.google.com/identity/passkeys
Microsoft	Azure Identity Management and access control security best practices: https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices
FIDO Alliance	The FIDO Alliance is a leader in the change to phishing-resistant (passwordless) authentication: https://fidoalliance.org/fido2/

Industry Best Practices Related to Multi-factor Authentication	
Reference	Description
Center for Information Security (CIS)	CIS has developed and published the CIS Controls framework to provide organizations with a process to design, implement, measure, report, and manage enterprise security. The following CIS control categories provide guidance related to MFA: Control 5: Account Management Control 6: Access Control Management Control 14: Security Awareness and Skills Training
National Institute of Standards and Technology (NIST)	NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. NIST has developed Special Publication 800-63B for Digital Identity Guidelines related to Authentication and Lifecycle Management. The following NIST 800-63B guideline sections provide suggestions related to MFA: Section 4 - Authenticator Assurance Levels Section 5 - Authenticator and Verifier Requirements Section 6 - Authenticator Lifecycle Management Section 10 - Usability Considerations by Authenticator Type
Gartner Peer Insights, User Authentication Software Reviews	Gartner lists vendor products, including reviews and rating information, to assist companies with identifying and researching tools that fit specific use cases. Refer to the following to view Gartner's User Authentication Reviews and Ratings: User Authentication Reviews and Ratings

Vulnerability Management

Vulnerability Management for Apple Suppliers

Exploiting vulnerabilities remains a primary method of enterprise infiltration for threat actors. Consequently, Apple suppliers must prioritize vulnerability management. This comprehensive process involves identifying, assessing, remediating, and reporting security vulnerabilities within networks, systems, and applications. By adopting a holistic vulnerability management approach and integrating it with other data security measures, Apple suppliers can significantly reduce their attack surface and protect Apple data.

Vulnerability Management Guidance for Apple Suppliers

The approach and tools used to manage vulnerabilities will vary based on organizational size and the associated risks of systems and applications. At a minimum, suppliers are expected to implement a vulnerability management program that incorporates the following within their environments:

Asset Management

An asset register containing detailed information about information systems should be maintained to track and report on assets throughout their lifecycle. A comprehensive asset register is crucial for ensuring that all systems and applications are included in the organization's vulnerability management scope.

An asset that has access to or is connected to the enterprise network should be registered within an asset inventory system. Assets can include, but are not limited to: network devices; endpoints; infrastructure; hosts; services; software; and applications.

The asset inventory system should be maintained to keep track of the following information for each asset:

- an assigned asset owner
- the asset location
- the asset registration date
- a mechanism for alerting in the case of a missing asset

Asset owners should review asset registration data annually and after significant changes to maintain accuracy. The asset management system should also facilitate the transfer of asset ownership when teams change, ensuring timely updates.

Vulnerability Identification and Remediation

A process to perform internal and external vulnerability scans should be in place to identify and remediate vulnerabilities present in internally-facing and internet-facing systems and applications. Apple requires its suppliers to implement the following:

- Vulnerability scans should be performed on all systems and applications at least quarterly, including (but not limited to) servers, network devices, peripheral devices, and workstations.
- Internal vulnerability scans should be performed on internal-facing systems.
- External vulnerability scans and penetration tests should be performed on internet-facing systems. Such penetration tests should be conducted at least annually.
- Internally-developed applications should adhere to Open Web Application Security Project (OWASP) Top Ten secure coding guidelines throughout development, with regular code review scans to identify any code-related vulnerabilities.
- Both internally-developed and third-party applications should undergo application vulnerability scanning and penetration testing.

Apple suggests that vulnerability scanning tools be configured with the following:

- Vulnerability scans are credentialed (authenticated).
- Scanning policies are configured to identify vulnerabilities relevant to the types of systems being scanned.
- The Vulnerability Signature Database[2] is automatically updated from vendor releases.

A process should be in place to remediate vulnerabilities identified as a result of vulnerability scanning. A pre-established vulnerability risk matrix with corresponding remediation timelines should be defined based on the risk that the system or application presents to the organization. Apple requires its suppliers to align to the following vulnerability remediation timelines:

- critical vulnerabilities (CVSS 9.0 - 10.0) remediated within 30 days of identification (Note: external vulnerabilities remediated within 72 hours of identification)
- high vulnerabilities (CVSS 7.0 - 8.9) remediated within 90 days of identification
- medium vulnerabilities (CVSS 4.0 - 6.9) remediated within 180 days of identification
- low vulnerabilities (CVSS 0.1 - 3.9) should have an established timeline for remediation; recommendation within one year remediation; recommendation within one year

Suppliers are recommended to have procedures in place to log and track any vulnerabilities that cannot be remediated.

[2] A vulnerability signature is a representation of the vulnerability language.

Patch Management

A process to test and implement updates and patches in accordance with defined vulnerability remediation timelines should exist to ensure these tools do not become susceptible to vulnerabilities and potential exploitation.

A patch management policy should exist and establish guidelines for analyzing, testing, and implementing updates and patches to systems and applications. Patches should be applied to systems and applications on a pre-established cadence based on the risk that the system or application presents to the organization. Procedures to escalate implementation of patches to address zero-day vulnerabilities should also be defined. Any systems or applications that can no longer receive patches or updates should be considered end-of-life (EOL). Any EOL systems or applications should be replaced or upgraded to a manufacturer-supported version prior to reaching EOL. If an EOL system or application cannot be replaced or upgraded prior to reaching EOL, these systems and applications should be tracked in an asset register.

Industry Best Practices Related to Vulnerability Management

The table below references articles and benchmarks containing industry best practice guidance related to vulnerability management.

Industry Best Practices related to Vulnerability Management	
Reference	Description
Center for Information Security (CIS)	CIS has developed and published the CIS Controls framework to provide organizations with a process to design, implement, measure, report, and manage enterprise security. The following CIS control categories provide guidance related to vulnerability management: Control 1: Inventory and Control of Enterprise Assets Control 2: Inventory and Control of Software Assets Control 7: Continuous Vulnerability Management
National Institutes of Standards and Technology (NIST)	NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. These NIST special publications provide suggestions related to vulnerability management: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology 800-115: Technical Guide to Information Security Testing and Assessment 1800-5: IT Asset Management
United States Computer Emergency Readiness Team (US-CERT)	US-CERT is a branch of the United States Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center. US-CERT has developed the Cyber Resilience Review (CRR) as a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The following CRR assessments provide guidance related to vulnerability management: Volume 1: Asset Management Volume 4: Vulnerability Management

Incident Management

Incident Management for Apple Suppliers

In addition to having an Information Security program, a dedicated Security Response team (SIRT) that is well-versed in preparing for, detecting, analyzing, containing, eradicating, and recovering from threats, both internal and external, is integral to minimizing the risk or impact of a security breach.

Incident Management Guidance for Apple Suppliers

Apple recommends suppliers have an incident management program in place with the following capabilities:

Preparation

Suppliers should ensure the following to be adequately prepared for responding to incidents:

- Have a plan: Suppliers should develop and implement an incident response plan to follow when a security incident occurs. This plan should use a risk-based approach and incorporate input from business units across the organization. Apple recommends including the following in the incident response plan:
  - defined roles and responsibilities for each phase of incident response
  - defined incident alert notification mechanisms and procedures
  - incident response process flows or procedures that include steps for preparation, detection and analysis, containment, eradication, and recovery
  - defined incident criteria and incident classification
  - communication and notification protocols (for example, breach notification requirements)
  - identification of requirements for the remediation of any identified weaknesses in information systems and associated controls
  - requirements for periodic testing (such as tabletop exercises), at least annually, of the Incident Response Plan to validate effectiveness
- Assign responsibilities: Suppliers should establish a dedicated incident response team or an individual directly responsible for security incident response, with the necessary skills, knowledge, and expertise to handle security incidents effectively. Contact information (a group email address at minimum) for the individual(s) responsible for security incident response should be shared with Apple as part of the preparation phase of the incident response process. Given the significant time and effort involved in

incident response activities, suppliers could evaluate the option of outsourcing these tasks to managed services or third-party providers.

- Know your assets: Suppliers should compile a list of information technology (IT) assets such as networks, servers, and endpoints. Each asset should be evaluated based on its risk to the organization, including identification of assets that are business critical or hold sensitive data.
- Get your tools and technologies ready: Preparing and deploying the necessary hardware and software for incident response is key during the preparation phase. These tools may include security information and event management (SIEM) systems, incident response platforms, forensic tools and dedicated computers, and storage devices.
- Prepare your employees: Employees and contractors should undergo training that provides awareness related to information security best practices. Training should include identification and prevention of common information security threats.

Detection and Analysis

Upon detection of an incident, the individual directly responsible for security incident monitoring and analysis should immediately log information about the incident including, but not limited to:

- incident start date and time
- how the incident was identified
- whether or not the incident is ongoing
- how the incident was/is contained (if contained)
- signs of persistence on the network
- signs of lateral movement on the network
- data that was disclosed during the incident, including any data that was exfiltrated, and any Apple data disclosed or accessed during the incident
- root cause of the incident

This information should be used to communicate the nature of the incident to management, staff, affected third parties, and if necessary, Apple. Responses to questions posed by Apple about a reported security incident should be provided as soon as practical. If a response is expected to take longer than eight hours, suppliers are expected to provide Apple awareness of that situation.

Suppliers should implement tools and processes that enable information security professionals to have visibility into any internal or external threats posed to the organization and perform analysis activities as needed. Potential activities to accomplish this may include:

- Leveraging detection and response tools on endpoints or network intrusion prevention and/or detection systems. Although anti-virus should be used, this is a baseline information technology hygiene function, and not a replacement for intrusion detection systems.
- Employing a centralized monitoring approach using a tool that aggregates logs and alerts from all systems and applications across the organization into one centralized view.

Containment, Eradication and Recovery

- Containment: Upon confirmation of a security incident, an incident containment strategy should be implemented to stop the attack before it causes additional damage. The containment strategy should consider the level of damage the incident can cause, the need to keep critical services available to employees and customers, and the duration — a temporary solution for a few hours, days or weeks, or a permanent solution.
- Eradication: In this critical stage, suppliers should focus on completely removing the presence of the identified threat or attacker from the affected systems. The main objectives of the eradication phase are to identify the root cause of the incident, remove the malicious code or access points, repair any vulnerabilities, restore affected systems to a known good state, and implement necessary security measures to prevent future occurrences.
- Recovery: Once the threat is eradicated, restore systems and recover normal operations in a timely manner. This involves activities such as system reconfiguration, data restoration, and validating the integrity of affected systems.

Post-Incident Activity and Lessons Learned

After an organization responds to an incident and operations are no longer disrupted, it is best practice to conduct a post-incident review to consider the performance of response activities. Companies can use this review to understand why an incident or series of incidents occurred and what the organization can do prevent them in the future. The review should consider:

- What happened and when?
- How well did the incident response team respond to the incident?
- What information was needed sooner?
- Have we learned how to prevent similar incidents in the future?
- Have we discovered new precursors or indicators of similar incidents to watch for in the future?
- What additional tools or resources are needed to help prevent or mitigate similar incidents?

The results of the post-incident review stage should be incorporated into the organization's incident response plan to improve incident response capabilities.

Industry Best Practices Related to Incident Management

The table below references articles and benchmarks containing industry best practice guidance related to incident management.

Industry Best Practices related to Incident Management	
Reference	Description
Center for Internet Security (CIS)	CIS has developed and published the CIS Controls framework to provide organizations with a process to design, implement, measure, report, and manage enterprise security. The following CIS control category provides guidance related to security incident management: Control 17: Incident Response Management
National Institutes of Standards and Technology (NIST)	NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. This NIST special publication provides suggestions related to vulnerability management: 800-61: Computer Security Incident Handling Guide
SANS Institute	The SANS Institute's ongoing mission is to empower cybersecurity professionals with the practical skills and knowledge needed to make our world a safer place. The following handbook provides guidance related to security incident management: Incident Handler's Handbook
United States Computer Emergency Readiness Team (US-CERT)	US-CERT is a branch of the United States Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center. US-CERT has developed the Cyber Resilience Review (CRR) as a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The following CRR assessment provides guidance related to security incident management: Volume 5: Incident Management

For any security events affecting Apple data or Apple systems, contact the Apple Security Incident Response Team (SIRT) within eight hours of identification:

sirtnotify@apple.com
+1-408-862-0200

Security Awareness Training

Security Awareness Training for Apple Suppliers

While employees are an organization's greatest asset, they are also the asset most susceptible to a cyber attack. Most breaches that occur involve a human element — honest mistakes made by employees — that can be mitigated by security awareness training. Implementation of an effective security awareness training program addressing the cybersecurity mistakes that employees often make when performing their job duties can help to minimize risk and prevent the loss of sensitive data, capital, and/or brand reputation.

Security Awareness Training Guidance for Apple Suppliers

Apple requires that suppliers implement a security awareness training program applicable to all personnel (employees, contractors, etc.). The program should regularly evaluate the personnel's understanding of information security concepts, governance (that is, policies and standards), and expectations regarding their responsibilities.

Apple recommends that suppliers consider the following when implementing a security awareness training program:

- Frequency: Security awareness should be evaluated when a new employee is hired and re-evaluated at least annually thereafter, as well as upon a personnel's role change.
- Acknowledgement: Training should capture documented acknowledgement from employees, confirming their understanding and accepting their responsibilities outlined in the training.
- Tracking: Training completion should be tracked for all personnel to validate that training was completed within the period defined by company policy.
- Evaluation: Training curriculum should be reviewed and updated periodically to reflect current threats and incorporate updates in security policies and procedures to ensure personnel are informed with the latest industry trends.
- Information security concepts: Training curriculum should incorporate current information security concepts, including, but not limited to:
  - security policies and procedures
  - acceptable use of systems and applications (of example, internet, email, and company assets)
  - proper password usage

    - data backups
    - keeping software and applications updated with security patches
    - recognizing and reporting social engineering attacks
    - proper antivirus protection
    - reporting suspected incidents or violations of security policy
- Regulatory requirements: Suppliers that provide products or services that must comply with regulatory requirements such as the Payment Card Industry (PCI) and Health Insurance Portability and Accountability Act (HIPAA) are required to implement security awareness programs.
- OWASP Top Ten: Software development suppliers should provide development-specific training that is aligned with industry best practices, such as Open Web Application Security (OWASP) Top Ten.

In addition to a security awareness training program, suppliers should consider conducting periodic campaigns that simulate social engineering attacks in order to train personnel to detect and report attacks.

Apple suppliers that have access to Apple's network and systems may be in scope for Apple's prescribed security awareness training, which must be completed by the assigned deadline.

Industry Best Practices Related to Security Awareness Training

The table below references articles and benchmarks containing industry best practice guidance related to security awareness training.

Industry Best Practices Related to Security Awareness Training	
Reference	Description
Center for Internet Security (CIS)	CIS has developed and published the CIS Controls framework to provide organizations with a process to design, implement, measure, report, and manage enterprise security. The following CIS control category provides guidance related to security awareness training: CIS Critical Security Control 14: Security Awareness and Skills Training

Industry Best Practices Related to Security Awareness Training	
Reference	Description
Cybersecurity & Infrastructure Security Agency (CISA)	The CISA created the Cybersecurity Awareness Program as a national public awareness effort aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. CISA Cybersecurity Awareness Program
National Institute of Standards and Technology (NIST)	NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. The following NIST Special Publications provide suggestions related to security awareness training: 800-50: Building an Information Technology Security Awareness and Training Program
OWASP Top 10	The Open Web Application Security (OWASP) Top Ten is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.
SANS Institute	The SANS Institute's ongoing mission is to empower cybersecurity professionals with the practical skills and knowledge needed to make our world a safer place. The following portal provides resources and guidance for building and maturing a security awareness training program: Build and Mature Your Security Awareness Training Program
United States Computer Emergency Readiness Team (US-CERT)	US-CERT is a branch of the United States Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center. US-CERT has developed the Cyber Resilience Review (CRR) as a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The following CRR assessment provides guidance related to security awareness training: Volume 9: Training and Awareness
Cyber Readiness Institute	The Cyber Readiness Institute (CRI) is a non-profit organization aimed at helping small- to medium-sized businesses (SMBs) become more secure against today's most common cyber vulnerabilities. As a member and co-chair of the CRI, Apple partnered with the CRI to develop a free Cyber Readiness Program to provide Cyber Leaders guidance for building foundational cyber security practices within their organizations. Cyber Readiness Program - Apple suppliers should register with the Champion Referral Code "APL23"

Event Logging

Event Logging for Apple Suppliers

Event log data contains records of events that occur inside a system or application and are generated by many sources, including applications, security software, and operating systems. Event logging provides an audit trail used to diagnose, understand, and reconstruct system and application problems. Logs are also useful for establishing baselines, identifying operational trends, and supporting internal investigations (such as forensic analysis). While all event logs are integral to tracking activity occurring in a system or application, capturing and analyzing security-related event logs is a critical part of information security management, because these logs help security personnel understand if a vulnerability exists and help prevent or reduce the impact of a security breach.

Event Logging Guidance for Apple Suppliers

Apple recommends that suppliers implement event logging for all systems and applications that are capable of producing security-related event logs. This includes systems and applications hosted in a cloud environment managed by the supplier.

Types of Events

The types of event logs captured will vary depending on the size of the organization, as well as the systems and applications that the organization uses. At a minimum, suppliers are expected to capture security-related event logs, including, but not limited to:

- administrative access logs
- anomalous event logs
- application errors
- authentication logs
- authorization logs
- HTTP activity
- system errors
- termination logs
- user access permission logs

Event Data

Each event log should contain information that describes the event, including, but not limited to:

- date/time
- unique identifier
- brief description of the event
- event category (denial of service, virus intrusion, physical access violation, etc.)
- asset(s), service(s), user(s), and/or organizational unit(s) triggering the event

Don't Log Sensitive Data

Suppliers should not log personally identifiable information (PII) or other sensitive data in plain text. When correlating information is needed for logging purposes, hashing sensitive data into identifiers is the preferred method.

Event Log Management Considerations

Apple suggests the following considerations when implementing event log management:

- Centralized event logging: Depending on the size of environment (that is, number of systems and networks), suppliers should consider implementing a centralized log management platform. This enables aggregation of logs from a multitude of sources across environments into a centralized repository to ease monitoring, auditing, and reporting on events. The log management platform should be synchronized with a Network Time Protocol (NTP) server and backed up regularly.
- Log alerting, monitoring, and auditing: Suppliers should designate an individual or team(s) responsible for monitoring and auditing security-related event logs. The responsible individual(s) should understand how to detect and respond to a suspicious log. Manual reviews of logs should be performed regularly, and event alerts should be enabled where applicable. Note that some regulatory requirements dictate that logs be reviewed at a certain frequency (that is, daily).
- Log protection: Access to log files and configurations must be restricted to only those with a specific role-based need. Modifications made to log file configurations must only be performed by authorized personnel.
- Log retention: Suppliers are recommended to keep immediately accessible active logs [hot] for 90 days minimum, and required to keep archived logs [cold] for two years minimum.

Industry Best Practices Related to Event Logging

The table below references articles and benchmarks containing industry best practice guidance related to event logging:

Industry Best Practices related to Event Logging	
Reference	Description
Center for Internet Security (CIS)	CIS has developed and published the CIS Controls framework to provide organizations with a process to design, implement, measure, report, and manage enterprise security. The following CIS control category provides guidance related to event logging: Control 8: Audit Log Management
National Institutes of Standards and Technology (NIST)	NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. The following NIST special publication provides suggestions related to event logging: 800-92: Guide to Computer Security Log Management
SANS Institute	The SANS Institute's ongoing mission is to empower cybersecurity professionals with the practical skills and knowledge needed to make our world a safer place. The following handbook provides guidance related to event logging: Creating a Logging Infrastructure
United States Computer Emergency Readiness Team (US-CERT)	US-CERT is a branch of the United States Office of Cybersecurity and Communications' National Cybersecurity and Communications Integration Center. US-CERT has developed the Cyber Resilience Review (CRR) as a non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The following CRR assessment provide guidance related to event logging: Volume 5: Incident Management

For any security events affecting Apple data or Apple systems, contact the Apple Security Incident Response Team (SIRT) within eight hours of identification:

sirtnotify@apple.com
+1-408-862-0200

Security Resilience

Security Resilience for Apple Suppliers

Security resilience is crucial for anticipating, withstanding, and rapidly recovering from ransomware attacks. Ransomware is a type of malware that encrypts a victim's data with the attacker demanding a "ransom," or payment, to restore access to files, networks, and systems.

Security resilience and ransomware response strategies are essential for protecting sensitive information such as personal data, intellectual property, and financial information. They also help ensure critical business functions can continue uninterrupted in the face of a ransomware attack.

Security Resilience Guidance for Apple Suppliers

Apple recommends that suppliers consider the following when implementing a security resilience strategy to withstand or quickly recover from ransomware attacks:

Establish Ransomware-specific Incident Response and Business Continuity Plans:

Incident response plans must address ransomware attacks explicitly, incorporating early detection methods to prevent data encryption and outlining strategies for continued operations during and after an attack. Suppliers should consider the following when developing these plans:

- Establish crisis management resources: Pre-identify security and recovery experts with designated responsibilities for ransomware incidents. Consider external consultants as needed. Create internal and external communication channels for timely information sharing, and control information flow through a centralized collection and dissemination process.
- Implement detection and response tools: Deploy endpoint and network-level detection and response controls capable of identifying suspicious ransomware behavior and halting encryption or data theft attempts
- Conduct continuous evaluation: Regularly conduct tabletop exercises to refine ransomware response plans and learn from real-world incidents. Develop procedures for managing resilience activities, and investigate effective resilient response strategies. Promptly address testing and monitoring findings by updating policies and procedures. Resilience should be an ongoing process, with plans updated in response to security incidents, business continuity events, and system changes.

Backups and Recovery:

Regular backups of all critical data are essential for swift recovery from ransomware attacks. These backups should be stored offline and accessible across both on-premises and cloud environments. Consider the following backup and recovery strategies:

- Isolated and offline backups: Implement a data backup and recovery model that includes isolated backups that aren't reachable/accessible from the core corporate environment without making infrastructure changes and/or requiring numerous administrative authentication/authorization steps, and which cannot be accessed using the same authentication credentials as could be used to access any account or tool in the core corporate environment. This could be done by creating a new network segment for the backups, with a deny-all firewall protecting the segment. The firewall rules are only opened when the data is needed or for replication. This is also referred to as air-gap storage.
- Immutable storage: Many major cloud providers now support object locking, also referred to as write once, read many storage or immutable storage. Implement a backup solution that integrates seamlessly with this object lock feature to create immutable backups. Some backup solutions also offer policy-based scheduling for retention time periods and migration as needed
- Adhere to 3-2-1 backup rule: Maintain at least three copies on two media types for backups, with one copy stored at an offsite location. Common combinations include disc and cloud, network-attached storage and cloud, or disk and tape.

Industry Best Practices Related to Security Resilience

The table below references articles and benchmarks containing industry best practice guidance related to security resilience:

Industry Best Practices related to Security Resilience	
Reference	Description
Cybersecurity & Infrastructure Security Agency (CISA)	CISA collaborates with industry to build more secure and resilient infrastructure for the future. The Cyber Resilience Review (CRR) is a no-cost, non-technical assessment to evaluate operational resilience and security practices. The CRR assesses programs and practices across a range of 10 domains, including risk management, incident management, service continuity, and others. CISA's Cyber Resilience Review Domains
National Institutes of Standards and Technology (NIST)	NIST is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. The following 2021 NIST special publication provides guidance on developing cyber-resilient systems and recovery planning: NIST SP 800-160 Vol. 2: Developing Cyber-Resilient Systems
Department of Homeland Security (DHS)	The United States officially recognized resilience in the most recent National Security Strategy, which states that the U.S. must enhance its resilience. DHS works with all levels of government, the private and nonprofit sectors, and individual citizens to make our nation more resilient to acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters. DHS: Resilience
Center for Internet Security (CIS)	CIS has developed and published the CIS Controls framework to provide organizations with a process to design, implement, measure, report, and manage enterprise security. The following CIS control category provides guidance related to cyber resilience: Control 11: Data Recovery

For any security events affecting Apple data or Apple systems, contact the Apple Security Incident Response Team (SIRT) within eight hours of identification:

sirtnotify@apple.com
+1-408-862-0200

Network Segmentation

Network Segmentation for Apple Suppliers

Many security breaches involve the use of pivoting, where threat actors utilize a system that they have already compromised as a launch point for attacks against additional systems or services that live in the same network, which may not have originally been reachable by an attacker. Flat network topologies (like the internet and corporate networks), and nearly flat network topologies (like the internet, demilitarized zones [DMZ], and corporate networks), are particularly susceptible to these types of attacks.

Network segmentation is a strategy for addressing risks, like pivoting, by creating boundaries between groups of systems of different risk levels, in order to limit communication between the groups — specifically, limiting the communication to only what is necessary to perform required business functionality. In addition to these preventative measures, network segmentation also provides logical chokepoints within an infrastructure that can be used for performing security monitoring in order to detect potential threats.

Network Segmentation Guidance for Apple Suppliers

Implementing network segmentation involves two steps: where network segmentation boundaries should be created, and how to implement them.

Where to Employ Network Segmentation

Fundamentally, network segmentation involves the principle of least privilege as applied at the network layer. As mentioned above, simplistic versions of this are boundaries between the internet and the corporate network, or between internet, DMZ, and the corporate network. Apple recommends that suppliers apply network segmentation at a more granular level. Factors to consider include:

- Sensitivity & risk of the system/service: One factor to take into consideration is the sensitivity/risk level of a type of system/service, which can include the data contained in the system, or the functions performed by the system. These should be viewed in the context of the availability, integrity, and confidentiality triad of information security. For example, an intranet home page should not contain highly sensitive proprietary manufacturing data., nor should it have the ability to shut down a set of hypervisors. Exposure of information contained on an intranet homepage should not be as catastrophic as exposure of data concerning the manufacture of non-public products. Similarly, downtime for a company intranet homepage should not be as disruptive as the loss of systems manufacturing products.

- Users of the system/service: Another factor to take into consideration are the users of a system and/or service. This should closely align with the functions above. Examples of questions to consider include: Does an external user need access to the management ports for your hypervisors? Similarly, does an internal finance office worker need that same access? Or does someone in Human Resources need access to a bespoke piece of manufacturing equipment? The answers to these questions should be "no."

Recommended network segmentation boundaries include:

- manufacturing networks (operational technology)
- system administration plane (for example, hypervisor administrative access)
- network administration plane (for example, making network/firewall changes)
- internal corporate network
- demilitarized zone (DMZ)
- guest network

How to Implement Network Segmentation

The first step is determining what to prioritize (that is, what should be segmented first). This should be based on the highest risks to the organization. Some important questions to consider include: What assets are the most important to protect? Where is the greatest risk for disruption and/or financial loss? Consider seeking consultation from a security service provider to go through this exercise.

Once the network boundaries and prioritizations are determined, the next step is to identify the network flows that are necessary to perform required business functionality. It is important to recognize that going through this exercise is a crucial step toward knowing your environment — not just for the purpose of limiting traffic, but also to detect and debug problems with system functionality, and even to be able to identify rogue traffic. Note that "solutions" like putting firewalls into "learning mode" in a production corporate environment don't necessarily yield these benefits, as it runs the risk of allowing malicious traffic through.

Some possible technical controls that can be used to implement network segmentation, either alone or in combination, include the following:

- physical networks
- firewalls
- network access controls (NAC)
- virtual private network (VPN)
- network overlays

In-depth coverage of the implementation of these technologies is beyond the scope of this document. However, one common factor that must be implemented, regardless of the technology used, is the concept of default deny ingress and egress. This means that all traffic should be blocked by default, and rules should be added to only allow the traffic that is necessary to perform the required business functionality. Doing the reverse — allowing all traffic and then using block lists of known exploits — is not as robust of a solution.

Industry Best Practices Related to Network Segmentation

The table below references articles and benchmarks containing industry best practice guidance related to Network Segmentation.

Industry Best Practices Related to Network Segmentation	
Reference	Description
Cybersecurity & Infrastructure Security Agency (CISA)	CISA works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future. Layering Network Security Through Segmentation
OWASP Top 10	The Open Web Application Security (OWASP) Top Ten is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. OWASP Network Segmentation Cheatsheet