October 2023

Supplier Security Guidance

Contents

Introduction	**1**
Multi-factor Authentication	**2**
Multi-factor Authentication for Apple Suppliers	2
Multi-factor Authentication Guidance for Apple Suppliers	3
Industry Best Practices Related to Multi-factor Authentication	4
Vulnerability Management	**6**
Vulnerability Management for Apple Suppliers	6
Vulnerability Management Guidance for Apple Suppliers	6
Industry Best Practices Related to Vulnerability Management	9
Incident Management	**10**
Incident Management for Apple Suppliers	10
Incident Management Guidance for Apple Suppliers	10
Industry Best Practices Related to Incident Management	14
Security Awareness Training	**15**
Security Awareness Training for Apple Suppliers	15
Security Awareness Training Guidance for Apple Suppliers	15
Industry Best Practices Related to Security Awareness Training	17
Event Logging	**18**
Event Logging for Apple Suppliers	18
Event Logging Guidance for Apple Suppliers	18
Industry Best Practices Related to Event Logging	20
Security Resilience	**21**
Security Resilience for Apple Suppliers	21
Security Resilience Guidance for Apple Suppliers	21
Industry Best Practices Related to Security Resilience	23

Introduction

This guidance is intended to highlight some of the key security areas that Apple suppliers are expected to implement. These measures, alone, are not 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 just rely on this guidance.

Please also note that the guidance here is not intended to reduce any obligations you have to Apple in your contract with 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. Complying with this guidance alone does not suffice to comply with those requirements, and in the event that anything in this guidance conflicts with those requirements, follow those requirements.

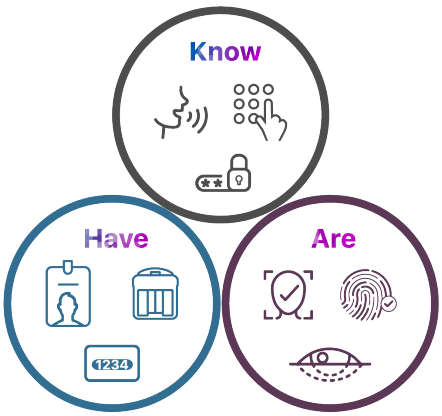
Multi-factor Authentication

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 commonly used type of authentication is the username and password combination. However, most hacking-related breaches involve guessing weak passwords or the use of lost or stolen credentials. A strong prevention against these type of attacks is the use of multi-factor authentication (MFA). There are three types of authentication factors. MFA is 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)
- Pin Number



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 susceptible to hijacking and phishing attacks.)
- Third-party Authenticator Application on a Trusted Device[1]. A downloaded authenticator application that lives on a user's trusted device and generates a one-time code required after the user enters their credentials.
- Hardware Token. A small physical key that is 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 (e.g. Touch ID)
- Facial recognition (e.g. Face ID)
- Retinal Scan (e.g. Optic ID)

[1]A trusted device is a device (e.g. 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. Check the 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 (e.g. administrative accounts, firewalls, routers, etc.)
- Any system that can access, process, transmit, or store Apple data

MFA doesn't stop there. 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 above 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 get around 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 be aware of developments in MFA technology.

The current gold standard in MFA is called Phishing-resistant MFA and relies on recently implemented standards called FIDO/WebAuthn authentication or Public Key Infrastructure (PKI)-based authentication. Apple, along with Microsoft and Google, has recently begun supporting these new standards. Refer to the index for helpful articles for implementing MFA.

Apple strongly recommends moving high-risk and critical systems to phishing-resistant MFA solutions where possible.

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/ 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/
Center for Information Security (CIS)	The 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

Industry Best Practices Related to Multi-factor Authentication	
Reference	Description
National Institute of Standards and Technology (NIST)	The National Institute of Standards and Technology (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 continues to be one of the most popular paths of enterprise infiltration for threat actors, so it's important for Apple suppliers to have a vulnerability management strategy.

Vulnerability management is a holistic process of identifying, evaluating, remediating, and reporting security vulnerabilities identified in networks and the underlying systems and applications. Implementing a holistic approach to vulnerability management (and combining it with other data security controls) is vital to minimizing Apple suppliers' attack surface and protecting Apple data.

Vulnerability Management Guidance for Apple Suppliers

The approach and tools used to manage vulnerabilities will vary depending on the size of the organization, and risks associated with the systems and applications used. At a minimum, suppliers are expected to implement a vulnerability management program that incorporates the following in their environment(s):

Asset Management

An asset register containing information systems should be maintained with sufficient detail to track and report on assets throughout their lifecycle. A well-maintained asset register is vital to ensure 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 revisit asset registration data at least annually and after significant changes to ensure it is kept up-to-date. The asset management system should also provide a mechanism or process to enable continuity of ownership such that, when an individual/

team no longer owns an asset, the ownership is updated to a new owner in a reasonable amount of time.

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

---

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

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

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)	The 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. The following 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 assessment provide guidance related to Vulnerability Management: Volume 1: Asset Management Volume 4: Vulnerability Management

Incident Management

Incident Management for Apple Suppliers

Threat actors actively attempt to access sensitive data, often targeting the supply chain to do so. A data breach can have significant financial and/or reputation impact on the supply chain. A dedicated information security team and program 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 (e.g. 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 table top 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 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.

Security events affecting Apple data or Apple systems should be reported to Apple's Security Incident Response Team (SIRT) within 48 hours of identification. The Apple SIRT can be notified through sirtnotify@apple.com or +1-408-862-0200.

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. It 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 ways 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)	The 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 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. The following NIST Special Publications provide suggestions related to Vulnerability Management: 800-61: Computer Security Incident Handling Guide
SANS Institute	The SANS Institute's ongoing mission is to empower cyber security 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 provide 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 48 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 that is most susceptible to a cyber attack. Breaches are often due to misinformed employees rather than an internal threat actor. 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

Suppliers that have access to Apple's network and systems are required to complete prescribed security awareness training on a periodic basis by the assigned deadline.

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 (i.e., 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.
- 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 the following:
    - Acceptable use of systems and applications (e.g. internet, email, and company assets)
    - Proper password usage
    - Data backups
    - Keeping software and applications updated with security patches

    - 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.

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)	The 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 Security Awareness Training: Control 14: Security Awareness and Skills Training
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 cyber security 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 provide guidance related to Security Awareness Training: Volume 9: Training and Awareness

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 as these logs help security personnel to 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 used by the organization. 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 (i.e., 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 should be 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 (i.e. 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 2 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)	The 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 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 Publications provide suggestions related to Event Logging: 800-92: Guide to Computer Security Log Management
SANS Institute	The SANS Institute's ongoing mission is to empower cyber security 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 48 hours of identification:

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

Security Resilience

Security Resilience for Apple Suppliers

Security resilience is crucial when it comes to anticipating, withstanding, and quickly recovering from ransomware attacks. Ransomware is a type of malware that encrypts a victim's data where the attacker demands for a "ransom", or payment, in order to restore access to files, networks, systems, etc.

Security resilience and ransomware response strategies help protect sensitive information such as personal data, intellectual property, and financial information, and ensure critical business functions can continue 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 should address ransomware attacks, implement early detection methods to prevent data encryption, and provide the ability to continue to operate in the event of a ransomware attack. Suppliers should consider the following when establishing incident response and business continuity plans:

- Prepare Crisis Resources: Identify security and recovery expertise in advance by designating personnel with specific responsibilities in the event of ransomware attacks. Retain third party consultants if needed. Establish internal and external communication channels to provide timely information. Manage the flow of information through the collection and dissemination of crisis-related information.
- Detection and Response tools: Implement endpoint detection and response security controls that can help detect suspicious ransomware-related behavior and could stop the encryption of sensitive files by an adversary.
- Continuous Evaluation: Perform yearly table top exercises, to proactively review plans for responding to ransomware attacks, or lessons learned to enable cross-domain learning from ransomware events. Develop procedures to detail when and where resiliency activities should be actively managed, and investigate successful strategies for resilient responses. Respond promptly to testing and monitoring results by updating specific policies and procedures to address any gaps or weaknesses. Resilience efforts should mature over time. Share operational information during each stage of a security incident or business continuity event to continuously enhance resilience. Then update plans when significant changes to systems or associated processes occur.

Backups and Recovery:

All critical data should be backed up regularly and stored offline so that it can be easily recovered in case of an attack. Critical data backups should be done both on local and cloud-based systems. Consider the following backup and recovery processes:

- 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.
- Consider 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
- Follow 3-2-1 Backup Rule: A backup strategy should, without fail, follow the 3-2-1 backup rule, which states an organization should have at least: 3 copies of their data, 2 media types for backups , and 1 backup stored in an off-site location. Some common 3-2-1 workflows combine disk and cloud, network-attached storage and cloud, and 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 works 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)	The 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 provide 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 48 hours of identification:

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