**AWS Security Policies**

To get started with these 20 AWS security policy templates, make sure your organization:

* Customizes the templates to meet your specific business needs and AWS environment
* Understands the limits of these templates, as the following list is not extensive
* Adds other relevant policies to your own information security program to fill gaps in this non-exhaustive list of policies
* Replaces all uses of [ABC Company] as a placeholder with the name of your organization

**Table of Contents**

[Background Check Policy 6](#_Toc72764844)

[Business Continuity Policy 8](#_Toc72764852)

[Change Management Policy 9](#_Toc72764856)

[Code of Conduct 10](#_Toc72764862)

[Configuration Management Policy 11](#_Toc72764863)

[Data Backup and Recovery Policy 13](#_Toc72764867)

[Data Security Policy 16](#_Toc72764883)

[Identity and Access Management Policy 20](#_Toc72764896)

[Incident Response Policy 22](#_Toc72764903)

[Information Security Policy 26](#_Toc72764913)

[Network Monitoring Policy 28](#_Toc72764920)

[Penetration Testing Policy 34](#_Toc72764942)

[Physical Security Policy 35](#_Toc72764948)

[Privacy Policy 37](#_Toc72764958)

[Risk Assessment Policy 38](#_Toc72764969)

[Security Awareness Training Policy 39](#_Toc72764975)

[Software Development Policy 41](#_Toc72764986)

[Vendor Management Policy 43](#_Toc72764993)

[Vulnerability Management Policy 45](#_Toc72764998)

# Background Check Policy

## Purpose

The purpose of performing background checks is to determine and or confirm, within appropriate legal and professional limits, the qualifications and suitability of a job candidate for the particular position for which the candidate is being considered.

## Scope

This procedure applies to all individuals who apply for employment with [ABC Company].

## Policy

### General

This policy will help ensure the safety of the public as well as a safe working environment at [ABC Company] and will help ensure that employment related decisions utilizing pre-employment criminal background checks are made in accordance with applicable law.

### Pre-Employment Considerations

[ABC Company] will perform pre-employment criminal background checks on all candidates for employment. In addition, if an employee changes positions within [ABC Company], an additional criminal background check will be performed. [ABC Company] complies with the federal and state laws in the jurisdiction in which [ABC Company] hires employees, federal and state equal opportunity laws and all other applicable legal authority that affects the performing of pre-employment criminal background checks. The results of a pre-employment criminal background check are confidential and are to be shared with members of [ABC Company] on a strict “need to know” basis.

### Definition

It is not the purpose of this policy to provide detailed information or descriptions of each individual pre-employment criminal background check that can be performed, as the specific methods/vendors used to acquire the information may change. It is not the purpose of this policy to provide detailed information on how to make a final decision regarding the results of a pre-employment background check; every case must be decided on its own merits subject to the Company requirement that all candidates be treated equally and consistently. It is not the purpose of this policy to provide detailed information of all applicable law. Questions about these subjects should be directed to [ABC Company] Executive Management.

### Background Check Guidelines

* Pre-employment criminal background checks are required for all candidates.
* All candidates will be required to sign appropriate authorizations and consents prior to performing of any pre-employment criminal background checks.
* Candidates that provide false or misleading information in their application process and/or authorization may be eliminated from any further consideration. Candidates are expected to provide accurate and complete information and not to omit material information needed to make a decision.
* Pre-employment criminal background checks must be completed before a candidate is offered a position. All job offers should be conditioned upon satisfactory completion of the pre-employment criminal background checks.
* All candidates shall be individually reviewed, and decisions shall be made with respect to employment based upon the totality of the candidate’s qualifications and the results of the pre-employment criminal background checks. The utilization of criminal records is generally a function of the nature of the criminal act, the length of time that has elapsed since that act and the nature of the job.
* In general, the relevance of a particular pre-employment criminal background check to a candidate’s eligibility for employment is based upon the following factors:
	+ The nature of the job for which the applicant is being considered;
	+ The nature of any adverse or negative information; including the particularly relevant facts surrounding the matter; and
	+ The age of any adverse or negative information; the age of the applicant at the time of the adverse incident in relation to the present may also be relevant.

# Business Continuity Policy

## Purpose

The purpose of this policy is to define the Business Continuity Program for ABC Company’s AWS environment. However, the detailed objectives, scope, limitations, and exclusions surrounding the program are documented in the Business Continuity Plan document, which expands upon the policies stated here.

The Business Continuity Program will enable a timely, effective response and recovery effort following a business or technology interruption to any key company location or process.  The various components of the Business Continuity Program include:

* Business Continuity Program Structure Definition
* Analysis
* Strategy Identification
* Strategy Implementation
* Training and Awareness
* Program Management & Maintenance

Business Continuity Program strategies and documentation (including this policy document) are reviewed on an annual basis and when significant changes occur within the organization.

## Scope

The Business Continuity Program addresses the operations at ABC Company. The scope of the Business Continuity Program includes the following key products and services hosted in the AWS environment.

## Policy

Business Continuity Program objectives include the following:

* Protecting the safety of employees and visitors
* Managing the threats and impacts associated with an interruption to critical operations, including a facility interruption or loss of resources (including personnel, technologies, and business partners).
* Reducing business continuity risk through four approaches:
	+ An appropriate and proactive control environment designed to decrease the likelihood of a disruptive event
	+ Strategies to effectively respond to a crisis
	+ Plans to recover critical business activities within stakeholder expectations
	+ The ability to maintain consistent communication with personnel and clients.

# Change Management Policy

## Purpose

The purpose of this policy is to establish proper procedures for changes/modifications to [ABC Company] information assets (IA) and AWS environment.

## Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and third parties that use [ABC Company] information assets or have access to the AWS environment. All information assets and information resources used by and in support of [ABC Company] business operations must comply with the provisions of this policy.

## Policy

### Documentation and Approval

The IT staff must obtain proper approval as well as document hardware and/or configuration changes to network devices.

* The [ABC Company] Change Management form is to be completed by IT and signed by [ABC Company] Executive management prior to the change. Information to be recorded on the form include, but are not limited to the following:
	+ Submitted By
	+ Approved By
	+ Date Planned
	+ Network Change Detail
	+ Test Plan
	+ Rollback Procedures
	+ Potential Negative Impact
	+ Security Impact

## Related Documents

[ABC Company] Change Management Form

# Code of Conduct

[ABC Company]’s rules and standards of conduct are essential to our productive work environment. All employees must familiarize themselves with company rules and standards; all employees will be held to them. Any employee who disregards or deviates from company standards may be subject to disciplinary action, up to and including termination of employment. While not intended to be an all-inclusive list, the examples below represent behavior that is considered unacceptable in the workplace. Behaviors such as these, as well as other forms of misconduct, may result in disciplinary action, up to and including termination of employment:

* Theft or inappropriate removal/possession of property
* Falsification of timekeeping records
* Possession, distribution, sale, transfer, or use of alcohol or illicit drugs in the workplace
* Fighting or threatening violence in the workplace
* Gossiping or spreading rumors about co-workers
* Boisterous or disruptive activity in the workplace
* Negligence or improper conduct leading to damage of company-owned or customer-owned property
* Insubordination or other disrespectful conduct
* Violation of safety or health rules
* Smoking in the workplace
* Sexual or other unlawful or unwelcome harassment
* Excessive absences or any absence without notice
* Unauthorized use of telephones, computers, or other company-owned equipment
* Unauthorized disclosure of any confidential information

Other forms of misconduct not listed above may also result in disciplinary action, up to and including termination of employment. If you have questions regarding [ABC Company]’s standards of conduct, please direct them to your supervisor. [ABC Company] seeks to create a positive work culture built on mutual respect and trust for coworkers and clients. Employees shall not gossip, complain, or otherwise engage in activities that are detrimental to these values. Any complaints or concerns with co-workers or clients should be communicated in a manner that fosters remediation of the underlying issues while preserving mutual respect and trust, involving appropriate members of management as necessary.

# Configuration Management Policy

## Purpose

[ABC Company] has established a formal policy and supporting procedures for developing configuration standards for system components that are consistent with industry-accepted hardening standards. This process will be conducted by authorized personnel with the appropriate technical knowledge and skill sets needed to undertake this activity. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding the company’s needs and goals.

## Policy

Configuration standards for system components utilize industry-accepted hardening standards. The list of industry-leading security standards, benchmarks and frameworks to utilize includes, but is not limited to, the following:

* Center for Internet Security (CIS)
* International Organization for Standardization (ISO)
* SysAdmin Audit Network Security (SANS) Institute
* National Institute of Standards Technology (NIST). Vendor-specific tools and checklists,

along with general setup and hardening procedures

* Amazon Web Services guidance

Additionally, when configuring system components, the following conditions must apply in order to ensure further compliance with industry standards.

* Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that the system configuration standards are consistent with industry-accepted hardening standards.
* Appropriately develop, implement, and adhere to relevant policies and supporting procedures to ensure that system configuration standards are updated as new vulnerability issues are identified.
* Appropriately develop, implement, and adhere to relevant policies and supporting procedures to ensure that system configuration standards are applied when new systems

are configured and verified as being in place before a system is installed on the network.

## Vendor Defaults

The following objectives are accomplished as part of AWS configuration:

* All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network.
* Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.

# Data Backup and Recovery Policy

This Data Backup and Recovery Policy is intended to ensure that the AWS environment is regularly backed up to prevent loss of data. All information stored in AWS is required to be backed up to keep it save in the event of system failure, disasters, or attacks. Information required to re-create the environment and services must be backed up including not only the data but operating system software, application software, information about contacts required to acquire new equipment, organizational financial account information, and information about the business function including procedures, policies, and processes. A copy of backup and recovery procedures must be stored away from the primary site so they are not destroyed in the event of a disaster.

**Purpose**

This Data Backup and Recovery Policy is designed to protect data in the AWS environment to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

**Scope**

This Data Backup and Recovery Policy applies to all equipment and data owned and operated by the organization. This policy is effective as of the issue date and does not expire unless superseded by another policy.

**Definitions**

*Backup*: The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

*Archive*: The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.

*Restore*: The process of bringing offline storage data back from the offline media and putting it on an online storage system such as a file server.

**Policy**

This Data Backup and Recovery Policy is an internal IT policy which defines the backup policy for the AWS environment which is expected to have its data backed up.

### Backup Identification

IT management is responsible for identifying all systems, vendor supplied programs including operating systems and application programs, IT policies, IT procedures, contact information for vendors and business partners and any other relevant information needed to rebuild the IT department from scratch in the event of a disaster. The business owners are responsible for identifying similar items required to rebuild their business function in the event of a disaster. The IT management working with the business owners must identify specific items relating to the business that must be backed up regularly and the frequency of backup. Any backups done on a slower schedule than documented in this policy must be agreed to in writing by the business owner and IT management.

IT management is responsible for creating procedures for transferring the identified items required for business rebuild offsite and ensuring they are transferred by delegated staff. IT management must be sure procedures exist and are kept both on and offsite for the purpose of both file recovery and disaster recovery.

### Timing

Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday. IT management is responsible for ensuring the backups are performed as scheduled. IT management delegates specific system administrators to perform specific backups and those administrators are responsible for carrying out that function but the IT managers must ensure that the administrators perform and check backups in a timely manner.

### Responsibility

The IT department manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for performing backups, testing backups, and test the ability to restore data from backups on a monthly basis.

### Testing

The ability to restore data from backups shall be tested at least once per month.

### Data Backed Up

Data to be backed up include the following information:

1. User data stored on the hard drive
2. System state data
3. The registry
4. Application software

Systems to be backed up include but are not limited to:

1. AWS environment
2. Production web server
3. Production database server
4. Domain controllers
5. Test database server
6. Test web server

### Archives

Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

### Restoration

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

### User Backup Responsibilities

Users are responsible for either storing their data on a networked file server rather than their local workstation or they must make arrangements for backing up their workstation or back it up on a regular basis. The frequency of backup and whether the data can be stored on a workstation depends on the business criticality of the data for preserving the business function. Storage of critical or sensitive data on a location other than a networked server must be approved by management.

### Other Backup Responsibilities

* Management must delegate someone to make periodic images of production servers for use to restore the server in the event of a catastrophic hardware failure or a disaster.
* The image should be stored offsite. Hardware requirements and specifications for all servers should be saved and stored offsite.
* Backup inventory must be tracked using implemented procedures. The locations of backup media must be known by delegated and authorized IT staff.
* Equipment used for restoration must be compatible with the backup media. This means that in the event of a disaster, backup reading equipment that is available must be capable of reading the backup media.
* All data and information required to rebuild the business including source code for developed programs, procedures, policies, software, system documentation, program documentation, network documentation, and contact information must be stored offsite.

### Enforcement

Since data preservation is important to maintain the organizational services, employees that purposely violate this policy may be subject to disciplinary action up to and including denial of access, legal penalties, and/or dismissal. Any employee aware of any violation of this policy is required to report it to their supervisor or other authorized representative.

### Other Requirements

* Files that are required to be backed up should be recorded for each server.
* Auditors should audit every six months to be sure all servers are being backed up regularly. Auditors must report results to senior management.

# Data Security Policy

**Purpose**

The purpose of this policy is to detail how confidential data should be handled within the AWS environment. This policy provides guidance on the use of confidential data and specific security controls to protect this data. Additionally, this policy will outline the company’s standards for use of encryption technology so that it is used securely and managed appropriately.

**Scope**

The scope of this policy covers all ABC Company confidential data, regardless of location.

**Policy**

***Use of Confidential Data***

The following applies to how users must interact with confidential data:

* Users must only access confidential data to perform his or her job function.
* Users must protect any confidential information to which they have been granted access and not reveal, release, share, email unencrypted, exhibit, display, distribute, or discuss the information unless necessary to do his or her job or unless the action is approved by his or her supervisor.
* Users must report any suspected misuse or unauthorized disclosure of confidential information immediately to his or her supervisor.
* If confidential information is shared with a third party, such as a contractor or vendor, a confidential information or non-disclosure agreement (NDA) must govern the third party’s use of confidential information.
* If confidential information is shared with a third party, the company must indicate to the third party how the data should be used, secured, and destroyed. Refer to the ABC Company Vendor Management Policy for additional guidance.

***Clean Desk***

Confidential data in printed form should not be left on desks unattended, unless in a locked office, and it should be removed from view when unsupervised.

***Security Controls for Confidential Data***

Confidential data requires additional security controls in order to ensure its integrity. ABC Company requires that the following guidelines are followed:

* Strong Encryption: Strong encryption must be used for confidential data transmitted internal or external to the company. Confidential data must always be stored in encrypted form, whether such storage occurs on a user machine, server, laptop, or any other device that allows for data storage.
* Network Segmentation: The company must use firewalls, access control lists, or other security control to separate the confidential data from wireless and or other unsecure network resources.
* Physical Security: Systems that contain confidential data, as well as confidential data in hardcopy form, should be stored in secured areas.
* Printing: When printing confidential data, the user should use best efforts to ensure that others do not view the information. Printers that are used for confidential data must be located in secured areas.
* Faxing: When faxing confidential data, users must use cover sheets that inform the recipient that the information is confidential. Faxes should be set to print a confirmation page after a fax is sent; and the user should attach this page to the confidential data if it is to be stored. Fax machines that are regularly used for sending and/or receiving confidential data must be located in secured areas.
* Emailing: Confidential data must not be emailed inside or outside the company without the use of strong encryption.
* Mailing: If confidential information is sent outside the company, the user must use a service that requires a signature for receipt of that information. When sent inside the company, confidential data must be transported in sealed security envelopes marked “confidential.”
* Discussion: When confidential information is discussed it should be done in non-public places, and where the discussion cannot be overheard.
* Redaction: Confidential data must be removed from documents unless its inclusion is absolutely necessary.
* Prohibited Storage: Confidential data must never be stored on non-company-provided machines (e.g., home computers).

***Examples of Confidential Data***

The following list is not intended to be exhaustive but should provide the company with guidelines on what type of information is typically considered confidential. Confidential data can include:

* Employee personal information, including social security numbers, medical, and healthcare information
* Consumer identifiable data in all forms, including but not limited to portfolio placement files and application databases
* Company financial data
* Network diagrams and security configurations
* Communications about corporate legal matters
* Passwords
* Bank account information and routing numbers
* Payroll information
* Credit card information

***Encryption Strategy***

The following represents the ABC Company encryption strategy:

* Manage logical access independently of native operating system access control mechanisms, if disk encryption is used. Decryption keys must not be tied to user accounts.
* Protect cryptographic keys used for encryption of confidential data against disclosure and misuse.
* Restrict access to cryptographic keys to the fewest number of custodians necessary.
* Store cryptographic keys securely in the fewest possible locations and forms.
* Generate strong cryptographic keys to protect confidential data.
* Secure cryptographic key distribution.
* Secure cryptographic key storage.
* Perform periodic cryptographic key changes.

***Encryption of Data at Rest***

Encryption of data at rest is required for storage of confidential data, such as any data located on company-owned or company-provided systems, devices, media, etc. This includes the following options for stored data:

* Whole disk encryption
* Encryption of partitions/files
* Encryption of disk drives
* Encryption of personal storage media/USB drives
* Encryption of backups
* Database encryption

***Encryption******of Data in Transit***

Encryption of data in transit is required to protect confidential data. This includes any data sent across the company network or any data sent to or from a company-owned or company-provided system. Types of transmitted data that can be encrypted include:

* FTP/SFTP file transfer
* Remote access sessions
* Web applications
* Email and email attachments
* Remote desktop access
* Communications with applications/databases

***Encryption Key Management***

The following guidelines apply to the ABC Company encryption keys and key management:

* Management of keys must ensure that data is available for decryption when needed.
* Keys must be backed up.
* Keys must be securely stored.
* Keys must never be transmitted in clear text.
* Keys are to be treated as confidential data.
* Keys must not be shared.
* Keys must be used and changed at minimum annually.

***Acceptable Encryption Algorithms***

Only the strongest types of generally accepted, non-proprietary encryption algorithms are allowed, such as AES or 3DES.

# Identity and Access Management Policy

**Purpose**

The purpose of this policy is to define the steps that must be taken within AWS to grant users and applications access in your AWS accounts. The permissions granted must be authenticated in an appropriate manner, in compliance with industry standards, and are given the least amount of access required to perform their job function.

**Scope**

The scope of this policy includes two types of identities: human identities and machine identities. AWS defines human identities as the administrators, developers, operators, and consumers of your applications that require an identity to access your AWS environments and applications. AWS defines machine identities as your workload applications, operational tools, and components require an identity to make requests to AWS services. This policy applies not only to employees, but also to external users with whom you collaborate and who interact with your AWS resources via a web browser, client application, mobile app, or interactive command-line tools. This policy also extends to machines outside of AWS that need access to your AWS environment.

**Policy**

### Identity Management

Apply the following best practices when managing human and machine identities:

* Rely on a centralized identity provider, which makes it easier to manage access across multiple applications and services.
* Leverage user groups and attributes to manage users as your AWS resources scales.
* Use strong sign-in mechanisms like MFA, password reuse policies, and strong password policies.
* Use temporary credentials through services like Amazon Cognito and with IAM roles.
* Audit and rotate credentials periodically to verify that the correct controls are in place.
* Store and use secrets securely through services like AWS Secrets Manager.

### Permissions Management

Permissions control who can access what, and under what conditions. Apply the following best practices when setting permissions for human and machine identities:

* Define permission guardrails for your organization using AWS Organizations.
* Grant access based on the principle of least privilege.
* Analyze public and cross-account access by attaching policies to resources or role assumption.
* Share resources securely when there is a need to share resources between separate accounts.
* Reduce permissions continuously by analyzing unused access, users, and roles through timestamp evidence.
* Establish an emergency access process for the unlikely event of an automated process or pipeline issue.

### CIS AWS Foundations Benchmark

The CIS has provided the industry with the AWS Foundations Benchmark to established best practices for AWS configurations. Apply the following CIS recommendations to your identity and access management practices:

* Avoid use of the root account.
* Ensure MFA is enabled for all IAM users.
* Ensure credentials unused for 90+ days are disabled.
* Ensure IAM password policies require at least 1 lowercase letter, 1 uppercase letter, 1 number, 1 symbol, and is at least 14 characters long.
* Ensure IAM password policies prevent password reuse.
* Ensure MFA is enabled for the root account, including hardware MFA.
* Ensure IAM policies are attached only to groups or roles.
* Maintain current contact details and register security contact information.
* Ensure IAM instance roles are used for AWS resource access from instances.
* Create a support role to manage incidents with AWS Support.
* Ensure IAM policies that allow full administrative privileges are not created.

# Incident Response Policy

**Purpose**

This policy is to ensure that [ABC Company] is prepared for a security incident within AWS if one were to occur. Even if you have appropriate preventive and detective controls, your organization should still implement an Incident Response Plan. The Incident Response Plan will enhance the ability of your team to operate effectively during an incident, to isolate and contain issues, and to restore operations.

**Scope**

The scope of this policy covers all information assets owned or provided by [ABC Company], whether they reside within the AWS environment or elsewhere.

**Policy**

### Plan Overview

[ABC Company] will ensure that the Incident Response Plan adheres to the following conditions:

* The Incident Response Plan includes, at a minimum, roles, responsibilities, and communication strategies in the event of a compromise.
* The Incident Response Plan includes specific incident response, business recovery and continuity procedures, and data backup processes.
* The Incident Response Plan includes coverage and response mechanisms for all critical AWS components and all other critical IT resources.

The Incident Response Plan is based on AWS best practice, which approaches incident response through the following four phases:

1. **Educate** your personnel about your AWS environment, cloud technologies, and how your organization uses them.
2. **Prepare** your incident response team to detect and respond to incidents in the AWS, and grant access to the necessary tools and AWS services.
3. **Simulate** both expected and unexpected security events within your AWS environment to understand the effectiveness of your Incident Response Plan.
4. **Iterate** on the outcome of your simulation and testing to improve your response activities, reduce time to identify and contain, and further reduce risk.

### Educate

Automated processes through AWS enable organizations to spend more time focusing on security measures. Automated incident response also makes it possible for your personnel to have the bandwidth to perform research and analysis, run practice tests, devise new response procedures, build new tools, and enhance their AWS skillsets.

### Prepare

All [ABC Company] employees should be aware of common security threats and incidents that may potentially compromise or cause harm to the organization’s AWS environment, or pose a significant financial, operational, or business threat to the organization as a whole. The Incident Response Plan should be viewed as a set of procedures for examining an AWS security incident, which includes preparing for, detecting, responding to, containing, recovery and any other necessary post-incident activities. The CSA states that there are 12 major cloud security risks, which include:

* Data breach
* Insufficient identity, credential, and access management
* Insecure UIs and APIs
* System vulnerabilities
* Account hijacking
* Malicious insiders
* Advanced persistent threats
* Data loss
* Insufficient due diligence
* Abuse and nefarious use of cloud services
* Denial of service
* Shared technology vulnerabilities

Per AWS recommendations, [ABC Company] will prepare for cloud security incidents through the following actions:

* Identify key personnel and external resource included on your incident response team.
* Develop incident management procedures.
* Pre-provision access to AWS for your incident response team.
* Pre-deploy tools into AWS to reduce the time from investigation to recovery.
* Prepare forensic capabilities to analyze evidence involved in an incident.

### Simulate

Once [ABC Company] has developed an Incident Response Plan that follows industry best practices and addresses cloud security risks, it’s time to test the plan. AWS says that these testing exercises are fundamentally about being prepared and iteratively improving your response capabilities. The value in simulation comes from:

* Validating readiness
* Developing confidence
* Following compliance obligations
* Generating artifacts accreditation
* Becoming faster and improving tools
* Refining communication and escalation
* Developing comfort with the unexpected

### Iterate

Any AWS incident deemed to be a relevant threat to the organization requires a rapid response from the incident response team. This rapid response follows a standard course of action designed to minimize the impact of the incident to the organization’s critical network and system infrastructure.

The following documented response mechanisms serve as the Standard Operating Procedures (SOP) for responding to any incident within the organization:

1. For any incident that has been detected, the incident response team is to be immediately notified.
2. The incident response team is to formally assume control and to identify the threat and its severity to the organization’s information systems.
3. In identifying the threat, the incident response team is to specifically identify which resources are at risk, both internal and external, and which harmful processes are currently running on resources that have been identified as *at risk*.
4. The incident response team is to make a determination if the resources at risk require physical or logical removal. Resources which pose a significant threat to the continuity of the business are to be immediately removed or isolated, either physically or logically.
5. If the incident has in any way resulted in a criminal matter that may be readily identified, [ABC Company] must immediately report it to law enforcement officials. This may include, but is not limited to the following:
* Local law enforcement
* The Federal Bureau of Investigation (FBI)
1. Investigating the incident is also a critical process within the Incident Response Plan. Proper investigative techniques are to include but are not limited to the following:
* Understanding how the incident occurred and what led to the compromise
* Reviewing all necessary system documentation, such as logs, audit trails, rule sets, configuration and hardening standards and all other supporting documentation
* Interviewing personnel as needed
* Examining any third-party providers and their respective products and services that are used within [ABC Company]’s AWS environment
* If warranted, a third-party resource for assisting in the investigation of the incident may be used (this will be done at the management’s discretion).

### CIS AWS Foundations Benchmark

The CIS has provided the industry with the AWS Foundations Benchmark to established best practices for AWS configurations. Apply the following CIS recommendations to your incident response practices:

* Ensure CloudTrail is enabled in all Regions.
* Ensure CloudTrail log file validation is enabled.
* Ensure the S3 bucket used to store CloudTrail logs is not publicly accessible.
* Ensure CloudTrail is integrated with CloudWatch.
* Ensure AWS Config is enabled in all Regions.
* Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket.
* Ensure CloudTrail logs are encrypted at rest using KMS CMKs.
* Ensure rotation for customer-created CMKs is enabled.
* Ensure VPC flow logging is enabled in all VPCs.

# Information Security Policy

**Purpose**

The purpose of this Information Security Policy is to provide a comprehensive framework for:

* Protecting the confidentiality, integrity, and availability of [ABC Company] information assets and the AWS environment.
* Protecting [ABC Company], its employees, and its clients from illicit use of [ABC Company] information assets and the AWS environment.
* Ensuring the effectiveness of information security controls over information assets and the AWS environment.
* Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related information security risks.
* Provide for development and maintenance of minimum controls required to protect [ABC Company]’s information assets and the AWS environment.
* Ensure that regular review of this manual is conducted at minimum annually or more frequently as needed.

**Scope**

These policies, procedures, standards, and guidelines apply to all employees, contractors, subcontractors, consultants, temporaries, guests, and third parties that use [ABC Company] information assets or the AWS environment. All information assets and information resources used by and in support of [ABC Company] business operations must comply with the provisions of this policy.

**Responsibility**

Responsibility for the policies contained in this manual are as follows:

* The [ABC Company] Chief Executive Officer is ultimately responsible for the policies contained within this manual and approval thereof.
* The President will inform all staff members of these policies upon initial approval as well as upon revision.
* All employees are responsible for reporting any violation of policy to the President.
* All members of management are responsible for the enforcement of [ABC Company] policies and procedures.
* All [ABC Company] employees are responsible for adherence to the policies contained within this manual.

**Policy**

### Employee Awareness and Acceptance

It is [ABC Company] policy to inform and educate employees on the importance of maintaining a secure environment and abiding by the policies as set forth in this manual. All employees must participate in Information Security Awareness training upon hire and annually thereafter. Training on these policies and procedures as well as additional safeguards, as selected by [ABC Company] Management are to be presented. All employees must sign an [ABC Company] Information Security Policy Manual Acknowledgment, attached as Appendix A of this manual prior to gaining unattended physical or logical access to [ABC Company] confidential information.

**Related Documents**

*[ABC Company] Training Procedure*

# Network Monitoring Policy

**Purpose**

The purpose of this policy is to establish the technical guidelines for network security monitoring and to communicate the controls necessary for a secure network infrastructure. The network monitoring policy will provide the practical mechanisms to support [ABC Company]’s comprehensive set of security policies.

**Scope**

This policy covers the AWS environment as well as IT systems and devices that comprise the corporate network or that are otherwise controlled by [ABC Company].

**Policy**

### Network Device Configuration

Network devices such as firewalls, routers, switches, and servers must follow the established [ABC Company] Password Policy as defined within this manual. Special considerations are to be made due to the nature of the device:

* Administrative (also known as “root”) access to systems is to be limited to only those who have a legitimate business need.
	+ Logging is to be enabled for all administrative user activities
* In addition to the guidance found within this policy, system hardening is to be performed using industry standard utilities and or resources:
	+ [Microsoft Baseline Security Analyzer](http://technet.microsoft.com/en-us/security/cc184924)
	+ [Center for Internet Security](http://benchmarks.cisecurity.org/downloads/browse/index.cfm?category=benchmarks.os.windows)
	+ [NSA Security Configuration Guides](http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml%22%20%5Cl%20%22microsoft)

### Event Logging

The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail the [ABC Company] requirements for logging and log review.

* Application Servers: At a minimum, logging of errors, faults, and login failures is required.
* Network Devices: At a minimum, logging of errors, faults, and login failures is required.
* Critical Devices: At a minimum, logging of errors, faults, and login failures is required.

### Log Review & Retention

The [ABC Company] IT team must perform log review at least once per month. Logs should be retained for online viewing going back 90 days and historically for a minimum of one year.

### Firewall Device Management

Internet connections and other unsecured networks must be separated from the company network through the use of a firewall.

### Firewall Configuration

The following statements apply to the company’s implementation of firewall technology:

* Firewalls must provide secure administrative access (through the use of encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.
* No unnecessary services or applications should be enabled on firewalls. The company should use hardened systems for firewall platforms or appliances (See System Hardening guidance above).
* Clocks on firewalls should be synchronized with the company’s other networking hardware using NTP or another means.
* The firewall ruleset must be documented and audited quarterly. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
* For its own protection, the firewall ruleset must include a “stealth rule,” which forbids connections to the firewall itself.
* The firewall must log dropped or rejected packets.

### Outbound Traffic Filtering

Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as “egress traffic filtering.”

[ABC Company] standard is outbound filtering enabling the following known “good” services to be permitted outbound from the network: 21, 22, 23, 25, 53, 80, 110, 443, and 995.

### Networking Hardware

Networking hardware, such as routers, switches, and access points, should be implemented in a consistent manner. The following requirements apply to the [ABC Company] implementation of networking hardware:

* Networking hardware must provide secure administrative access (through the use of encryption) with management access limited to only networks where management connections would be expected to originate.
* Clocks on all network hardware should be synchronized using NTP or another means
* Access control lists must be implemented on network devices that prohibit direct connections to the devices. Connections to the router should be limited to the greatest extent possible.
* Unused services and ports must be disabled on networking hardware.
* Access to administrative ports on networking hardware must be restricted to known management hosts and otherwise blocked with a firewall or access control list.

### Network Servers

Network servers should be implemented in a consistent manner. The following requirements apply to [ABC Company] network servers:

* Unnecessary files, services, and ports should be removed or blocked.
* Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
* A standard installation process should be developed for the company’s network servers.
* Clocks on network servers should be synchronized with the company’s other networking hardware using NTP or another means.

### Intrusion Detection/Intrusion Prevention

[ABC Company] requires the use of an Intrusion Prevention System (IPS) technology on critical or high-risk network segments.

* IDS procedures must be implemented to review and act on the alerts expediently.
* ISP procedures must be implemented that provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic. Also, if an IPS is used, it should be audited and documented according to the standards detailed in the “Firewalls” section of this document.

### Security Testing

Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the company’s network security. Security testing can be provided by IT Staff members formation Technology activities. The following sections detail the [ABC Company] requirements for security testing.

### Internal Security Testing

Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of the company’s IT team. Internal testing should not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network.

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the IT Manager. Internal testing should have no measurable negative impact on the company’s systems or network performance.

### External Security Testing

External security testing, which is testing by a third-party entity, is an excellent way to audit the company’s security controls. The IT Manager must determine to what extent this testing should be performed, and what systems/applications it should cover. External testing must not negatively affect network performance during business hours or network security at any time. [ABC Company] requires that external security testing be performed twice per year.

### Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the company’s network communications. When such assets are decommissioned, the following guidelines must be followed:

* Any asset tags or stickers that identify the company must be removed before disposal.
* Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
* At a minimum, data wiping must be used. Simply reformatting a device or deleting data is not an appropriate means of data destruction. If wiping is used, a tool designed to conduct a DoD compliant data wipe must be used, and the execution of the wipe should be logged. If physical destruction is used, a certificate of disposal or other evidence of destruction should be retained for audit purposes.

### Network Segmentation

By implementing network segmentation, [ABC Company] will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. The company requires the following with regard to network compartmentalization:

* Higher Risk Networks (Examples: Guest network, wireless network)
	+ Requirements: Segmentation of higher risk networks from the company’s internal network is required and must be enforced with a firewall or router that provides access controls.
* Externally-Accessible Systems (Examples: Email servers, web servers)
	+ Requirements: Segmentation of externally accessible systems from the company’s internal network is required and must be enforced with a firewall or router that provides access controls.

### Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the company’s IT staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable. The company requires that network documentation be performed and updated on a quarterly basis.

At a minimum, network documentation must include:

* Network diagram(s)
* System configurations
* Firewall ruleset
* IP Addresses
* Access Control Lists

### Antivirus/Anti-Malware

Computer viruses and malware are pressing concerns in today’s threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire company. [ABC Company] provides the following requirements on the use of antivirus/anti-malware software:

* All company-provided user workstations must have antivirus/anti-malware software installed.
* Workstation software must maintain a current “subscription” to receive patches and virus signature/definition file updates.
* Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually.
* In addition to the workstation requirements, virus and malware scanning must be implemented at the Internet gateway to protect the entire network from inbound threats.

### Software Use Policy

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. [ABC Company] provides the following requirements for the use of software applications:

* Only legally licensed software may be used. Licenses for the company’s software must be stored in a secure location.
* Open source and/or public domain software can only be used with the permission of the IT Manager.
* Software should be kept reasonably up to date by installing new patches and releases from the manufacturer.
* Vulnerability alerts should be monitored for all software products that the company uses. Any patches that fix vulnerabilities or security holes must be installed expediently.

### Maintenance Windows and Scheduled Downtime

Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the IT staff must perform the tasks during a scheduled weekly or monthly maintenance window. Tasks that are deemed “emergency support,” as determined by the IT Manager, should be done with one hour’s notice to users, or immediately if the situation dictates.

# Penetration Testing Policy

**Purpose**

The purpose of this policy is to protect the [ABC Company]’s AWS environment by setting standards for penetration testing.

**Scope**

This policy applies to the security of [ABC Company]’s AWS environment and information systems, including all company-owned or company-provided network devices, servers, personal computers, mobile devices, and storage media.

**Policy**

[ABC Company]’s AWS environment can be deployed in a way that is publicly-facing to the Internet, and therefore must be deployed in a way that eliminates vulnerabilities and protects against attacker exploits.

### Penetration Testing

Penetration testing (also called pen testing) is the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit. The test is performed to identify both weaknesses, including the potential for unauthorized parties to gain access to the system’s features and data, as well as strengths, enabling a full risk assessment to be completed.

* External and internal penetration shall be performed at least once a year.
* External and internal penetration shall be performed after any significant infrastructure or application changes.
* Penetration testing shall minimally consist of network-layer and application-layer penetration tests.
* Exploitable vulnerabilities noted during penetration tests shall be corrected and an adequate retest performed to demonstrate that identified exploit is addressed.

**Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action.

# Physical Security Policy

**Purpose**

The purpose of this policy is to protect the company’s physical information systems by setting standards for secure operations.

**Scope**

This policy applies to the physical security of [ABC Company]’s information systems, including, but not limited to, all company-owned or company-provided network devices, servers, personal computers, mobile devices, storage media, and the AWS environment.

**Policy**

### Limited and Monitored Physical Access

[ABC Company] maintains appropriate facility entry controls to limit and monitor physical access to [ABC Company] information assets and information resources.

All [ABC Company] users ensure that every physical access point is controlled during working hours and locked during non-duty hours and ensure that the following measures are taken with regard to the security of the building(s):

* Before securing the building/office ensure that all areas are vacated.
* Ensure that all lights and electrical appliances are switched off.
* Never leave the building/office via the fire exit (unless in the case of an emergency).
* Ensure that motion sensor alarms are activated.

### Environmental Controls

Environmental controls are implemented to protect all critical information assets. Critical information assets are provided a dry, climate-controlled environment. Additional controls include:

* Uninterruptable Power Supply (UPS)
* Battery-operated or electric stand-alone smoke detectors are installed
* Computing facilities undergo a periodic fire marshal inspection

### Physical Access to Network Devices

Only authorized personnel with a need-to-know shall be granted physical access to computing faculties. Network devices such as switches, routers, firewalls, and other appliances are kept in a locked room. Physical access to the room must be previously authorized by [ABC Company] Management and logged.

### Keys & Security Systems

Keys and systems access devices must be logged, and managed. Terminated employees must turn in their keys and leave the office area immediately. Supervisors should escort the employee from the office and ensure no [ABC Company] information assets or information resources are taken by the terminated employee. All applicable locks and security system codes should be changed as needed, based on [ABC Company] management guidance.

### Video Monitoring

The organization employs video surveillance of physical access to sensitive areas. These cameras shall be protected from tampering or disabling of the device. The results of the cameras shall be reviewed regularly and correlated with other entries and access control information, such as audit trails, sign-in sheets, authorization levels, and maintenance logs. The information from cameras shall be stored for at least three months in accordance with the organizations retention policy.

### Visitor Access

It is [ABC Company] policy to maintain the following visitor access controls:

* Use a visitor log to maintain a physical audit trail of all visitor activity.
	+ Log requirements include: visitor’s name, date and time of visit, the firm represented, and the onsite personnel authorizing physical access
	+ Retain this log for a minimum of three months, unless otherwise restricted by law.
* Upon validation of photo ID (government-issued driver’s license), Provide visitors with a temporary name badge or identifier to alert [ABC Company] employees
	+ Require visitors to turn in the temporary name badge or identifier prior to leaving.
* Ensure visitors are authorized access to areas where restricted data is stored or processed.

# Privacy Policy

**Purpose**

The purpose of this policy is to define how personally identifiable information, or PII, is to be collected, used, and protected by [ABC Company]. This policy also details what [ABC Company]’s legal requirements are regarding the privacy of personal data.

**Scope**

These policies, procedures, standards, and guidelines apply to all employees, contractors, subcontractors, consultants, temporaries, guests, and third parties that use [ABC Company] information assets or the AWS environment. All information assets and information resources used by and in support of [ABC Company] business operations must comply with the provisions of this policy.

**Policy**

[ABC Company]’s privacy policy should address the following aspects of protecting personal information:

* What personal information [ABC Company] collects from visitors and/or clients
* When [ABC Company] collects personal information
* How [ABC Company] uses personal information
* How [ABC Company] protects personal information
* How [ABC Company] uses ‘cookies’
* How [ABC Company]’s website complies with CalOPPA
* How [ABC Company]’s website complies with Fair Information Practices
* How to unsubscribe from [ABC Company]

# Risk Assessment Policy

**Purpose**

The purpose of this policy is to establish a formalized procedure for Risk Assessment Process in terms of information assets and information resources

**Scope**

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third-party that use [ABC Company] information assets or information resources. All information assets and information resources used by and in support of [ABC Company] business operations must comply with the provisions of this policy.

**Policy**

### Risk Assessment Scope

It is [ABC Company] policy to ensure that Risk Assessments are conducted to identify the critical assets that require protection, and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. Risk Assessments should take into account the potential adverse impact on the [ABC Company] reputation, operations, and assets.

### Annual Review

[ABC Company] will conduct an annual, formal Risk Assessment that identifies current and possible threats and vulnerabilities. [ABC Company] will review its policies, procedures, standards, and guidelines in accordance with the updated Risk Assessment and make any applicable modifications to counter evolving threats.

# Security Awareness Training Policy

**Purpose**

The purpose of the Security Awareness Training Policy is to ensure that [ABC Company] personnel possess the knowledge and attitude necessary to protect the physical and informational assets of the organization, including the AWS environment.

**Scope**

These policies, procedures, standards, and guidelines apply to all employees, contractors, subcontractors, consultants, temporaries, guests, and third parties that use [ABC Company] information assets or the AWS environment.

**Responsibility**

Below is the list of individuals (Security Awareness Team) who must be made aware of issues relating to security concerns. If all those listed have been consulted in regard to a security matter, [ABC Company] will be considered to be sufficiently safeguarded against those concerns as all systems, services, policies, and procedures will be in order or addressed to become in order as a result of consultation.

|  |  |
| --- | --- |
| **Role** | **Employee Name** |
|  |  |
|  |  |
|  |  |

**Policy**

### Email Reminders

There are times when the Security Awareness Team may wish to communicate or remind employees of the importance of security and the need to remain aware of security-related issues. The email notification will detail the systems, services, industry verticals, software, or hardware involved in the security event. Team Leads are required to take action and initiate any required changes in order to maintain security after receiving such notifications. Situations requiring a notification include when it has been determined that a security event may occur, if there are other warning signs in the industry of pending security threats, or when other security events have already occurred and have the possibility of targeting [ABC Company] services or systems.

### All-Hands Meetings

There are weekly Security Awareness meetings which have mandatory participation from Management, Development Teams, as well as other departments within [ABC Company]. During these meetings, we aim to identify possible security-related threats that may be involved with certain changes, or if certain changes require adjustment due to established or possible security threats. These will also serve as constant reminders to staff of the importance and awareness of security as a mindset required from everyone in the process of completing their duties.

### New Employee Onboarding

When an employee is onboarded, there is a mandatory review of the Information Security Policy and Code of Conduct. These two documents form the core of our security protocols and procedures and, hence, are deemed sufficient. This review of both documents is considered mandatory as a part of joining [ABC Company], and the employee must sign off their understanding of both documents before access to any systems is provided and before any work can be assigned.

### Annual Review

As a part of audit process, there will be an annual review of the Information Security Policy and Code of Conduct. This will be performed by the Security Awareness Team and will involve all Development Team members. Each person will sign off that:

* They have read and understand the Information Security Policy and Code of Conduct; and
* They understand the security requirements relevant to their Team

Any questions about any of the above will be addressed with the employee by a member of the Management Team. If any further clarification is required above that provided, it will be noted with the Security Awareness Team for further improvement to the documents and explanations provided.

### Security Awareness Training Content

Training content will consist of:

* Reviewing the Information Security Policy and addressing any questions about content or changes to the content
* Reviewing the Code of Conduct and addressing any questions about content or changes to the content
* Reviewing the security requirements and addressing any questions about content or changes to the content
* Sign-off by the employee for each of the above using the Security Awareness Acknowledgement Form

**Related Documents**

*Security Awareness Acknowledgement Form*

# Software Development Policy

**Purpose**

The purpose of this policy is to guide consistent and controlled development and modification of [ABC Company] software and system applications.

**Scope**

This policy applies to all employees, contractors, and third parties who are responsible for the development and management of software and system applications.

**Policy**

### Development/Test and Production Environments

The development/test environment and the production environment must be completely separated, meaning that testing is not allowed within the production environment. Both environments should be configured and secured based on industry-recognized standards. The duties of development/test personnel and production personnel must be documented and updated as necessary to ensure the segregation of duties.

### Software Development

Software development processes are required to include security throughout the software development lifecycle (SDLC) and must be based on industry-recognized standards to ensure security during the definition, design, analysis, and testing phases of software development. Software must be developed in compliance with regulatory requirements.

During the testing phase of development, operational databases containing sensitive data cannot be used. Test data must be removed from the test environment into the production environment prior to the deployment of code.

Developers must be trained in secure coding techniques, and training must be based on industry best practices and guidance. Processes for internal peer code review and custom application code review must be performed and documented.

*Security*

[ABC Company] must ensure via internal code review that applications are not vulnerable to injection flaws, buffer overflow, cryptographic storage, insecure communications, improper error handling, and high vulnerabilities. Web applications and application interfaces must not be vulnerable to cross-site scripting, improper access control, and cross-site request forgery. Public-facing web applications must be secured using either of the following methods:

* Manual or automated application vulnerability security assessments must be used to review public-facing web applications on at least an annual basis and following any changes.
* An automated technical solution that detects and prevents web-based attacks, such as a web-application firewall, must be installed to check traffic.

### Change Control

All changes to code, systems, and applications must be made in accordance with the Change Management Policy. Changes must be documented, approved, and communicated prior to implementation, and change control procedures should include processes for rollback, prioritization, systems interaction, and application and system owners. Version control must be enabled to log and track changes to code and applications.

# Vendor Management Policy

**Purpose**

The purpose of this policy is to establish a formalized procedure to ensure that current and potential IT vendors will be evaluated, selected, engaged, and managed in a consistent manner based on cost effectiveness, functionality/services risk, financial viability, and performance.

**Scope**

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and third parties that use [ABC Company] information assets or AWS accounts. All information assets and AWS accounts used by and in support of [ABC Company] business operations must comply with the provisions of this policy.

**Policy**

Because of cost, expertise, or ease, it may be necessary for [ABC Company] to engage the assistance of third-party service providers. This policy will help monitor the compliance-related risk associated with using third-party service providers. [ABC Company] will monitor all vendors’ compliance with SOC standards by obtaining and reviewing a copy of each vendor’s SOC 2 report on an annual basis.

**Responsibilities**

IT personnel will:

* Actively participate in the selection of vendors
* Maintain a list of IT vendors that affect financial data or confidential information
* Provide a list of IT vendors to the Disaster Recovery Administrator for Disaster Recovery evaluation and inclusion in the plan and inventory as appropriate
* When selecting a vendor, evaluate each material IT vendors’ cost effectiveness, functionality/services, risk, financial viability, compliance, and performance
* Consider the establishment or refinement of service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement
* Ensure contracts and agreements are in place ensuring the vendor’s compliance with legal and regulatory requirements and internal policies and procedures, that all service levels are agreed upon and documented clearly, and requiring the vendor to maintain the confidentiality of proprietary and confidentiality
* Manage relationships as follows:
	+ Treat strategic vendors as a partner. Communicate clearly and directly with them. As appropriate, help them understand our business, culture, processes, goals, priorities and expectations. Ensure roles and responsibilities are clear.
	+ If a vendor is not performing to our satisfaction, address the deficiencies by the following methods:
		- Verbal discussion of issues
		- Written communication outlining areas of improvement and clear expectations
		- Track performance expectations in measurable ways (service levels)
		- Put them on notice when the relationship is in jeopardy
		- Escalate issues to higher levels of Management in a timely manner

# Vulnerability Management Policy

**Purpose**

This document describes [ABC Company]’s requirements for maintaining up-to-date operating system security patches in the AWS environment and on all [ABC Company] owned and managed workstations and servers.

**Scope**

This policy applies to the AWS environment, workstations, or servers owned or managed by [ABC Company]. This includes systems that contain company or customer data owned or managed by [ABC Company] regardless of location.

**Policy**

The AWS environment, workstation, or servers owned by [ABC Company] must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by [ABC Company].