CONTACT Line - Availability Management

Version #1.0.0

- Created: Mon, 05 Jul 2021 13:09:28 -0400
- Last Modified: Mon, 05 Jul 2021 14:14:44 -0400

Introduction

This policy outlines the requirements CONTACT Line has set for themselves to ensure that services and systems which are provided to customers and that support critical business functions have the least amount of downtime as possible.

Follow the Policy

- Service delivery teams will use this as the standard for how services are delivered to customers.
- CONTACT Line system and service availability will be governed by this policy.

Availability Management

Availability management is the concurrent activities, plans, policies, procedures included in keeping systems and services available and running throughout their lifecycle.

As previously stated in the Information Security policy, the objectives of information security aim to preserve Confidentiality, Integrity, and Availability of information. Availability management activities at CONTACT Line will focus on the following high-level areas:

- Capacity Management
- Service Level Agreements
- Business Continuity Planning and Testing
- Disaster Recovery Planning and Testing

Capacity Management

The goal of Capacity management, in short, is to maintain peak performance with just enough resources.

CONTACT Line will continuously monitor resources, their performance, and future needs based on expected and actual business growth. A capacity management plan will be maintained which lays out how to maintain current capacity and what resources will be required as the CONTACT Line scales. The three following resources are the primary concern when implementing a capacity management plan:

- Data Storage Capacity
- Processing Capacity
- Communications Capacity

Infrastructure and resource provisioning must be flexible enough to add or remove resources required as often or as little as necessary. Flexibility requirements highlight how critical, continuous monitoring of resource usage and performance is to the availability of services and critical systems.

Annual budgeting will allocate enough to ensure that capacity can grow with the expected business growth, increased customer activity during peak times of the year, and other external factors that can cause sudden or prolonged resource strain.

Capacity management threats that can cause an exhaust of resources including but not limited to Distributed Denial of Service (DDoS) attacks will be addressed in relevant risk assessments no less than annually.

Service Level Agreements

Services being offered to customers will have signed service level agreements in place, in which the requirements for CONTACT Line will be listed. A service level agreement or SLA will answer the following questions:

- What services are being provided to the customer?
- What quality of service is the customer entitled to?
- What is acceptable downtime for the service?
- What metrics will be monitored to ensure service level commitments?

Metrics agreed upon in the service level agreements will be monitored and reported on to management periodically, and any significant deviation from a commitment made in SLAs will be addressed in due course.

Business Continuity Planning and Testing

Business continuity plans or BCPs are a set of documented processes and procedures which aim to keep services up and running in the event of an incident causing failure or impaired availability to a system, service or an entire core business function.

BCPs are activated during incidents that cause a disruption or failure of core business functions for the purpose of keeping services available for the duration of the failure.

BCPs are documented for each of the core business functions and systems that support them at CONTACT Line.

Detailed documentation that outlines the BCPs are located in procedures at CONTACT Line.

These plans are reviewed and revised to reflect any changes to changes to roles, responsibilities or core business functions and the systems that support them.

Business Continuity plans are test quarterly, when roles change and when significant changes to to CONTACT Line occur.

Disaster Recovery Planning and Testing

A disaster recovery plan or DRP, on the other hand, is a set of documented processes and procedures which aim to recover services to a state of permanence in the event of an incident causing failure or impaired availability to a system, service or an entire core business function.

DRPs are activated after the BCP is activated and its purpose is to recover to a state of permanence from incidents causing disruption or failure.

DRPs are documented for each of the core business functions and systems that support them at CONTACT Line.

Detailed documentation that outlines the DRPs are located in procedures at CONTACT Line.

These plans are reviewed and revised to reflect any changes to changes to roles, responsibilities or core business functions and the systems that support them.

Disaster Recovery plans are test quarterly, when roles change and when significant changes to to CONTACT Line occur.

CONTACT Line - Bring Your Own Device (BYOD)

Version #1.0.0

- Created: Mon, 05 Jul 2021 13:09:26 -0400
- Last Modified: Mon, 05 Jul 2021 14:15:59 -0400

Introduction

If you have permission to use your own personal device for CONTACT Line-related purposes, you must follow this policy.

It applies to all personal devices, that have been approved by the Security Team, you use to access CONTACT Line systems, software, or data.

Only secure devices are allowed to access the network, so notify the Security Team if you root (Android) or jail-break (iOS) your device.

Follow the Personal Device Approval Process

If you want to use your own device to access data on CONTACT Line networks, you must get approval from the Security Team.

The Security Team will ensure the device meets the requirements of all Information Security policies that apply to this device, such as:

- Encryption Policy
- Network Policy
- Endpoint Hardening Policy
- Acceptable Use Policy
- Password Policy

Use Your Device Appropriately

When you use your own device to access company-owned resources such as email, calendars, contacts, and documents, you must follow the same policies as when you use CONTACT Line devices. Here are some examples:

- If you use your device to store, send, or receive data, it must be legal and appropriate for the workplace.
- When you communicate through your device, you must always be respectful and follow CONTACT Line's Acceptable Use Policy.

Secure Your Device

When approving your device, the Security Team will ensure the device meets the following requirements:

- Limit access to workstations to only authorized users.
- Enable auto update on all devices for the operating system that is currently installed.
- Enable auto update on all software and applications that is installed on all devices.
- Ensure the device's storage is encrypted
- Enable the device to have its time and date automatically updated
- Set an inactivity timer on the device's display to turn on the screensaver or lock the screen after at least 5 minutes of inactivity.
- Ensure device requires a password, on boot, waking for sleep or after the screensaver is enabled
- Enable the built-in firewall or install the firewall used by your organization on all devices.
- Ensure password requirements are set on all devices if possible.
- Ensure a backup service is being utilized on all devices that are storing protected data.
- Ensure device has installed antivirus and is configured according to the Antivirus Policy.
- When leaving your device for any period of time, lock the screen or set it to sleep.
- Only licensed and software approved by the Security team is permitted to be installed on devices.
- Only licensed and software approved by the Security team is permitted to be installed on devices. Before applications or software is installed from Google Play Store, Apple App Store or other application stores it must be reviewed and approved by the Security Team.

Know Your Responsibilities and the Risks/Liabilities

It is your responsibility to:

- Back up your device's content, such as email, contacts, files, and media
- Pay all costs related to the device, including data and repairs
- Report lost or stolen devices to CONTACT Line and your mobility provider immediately
- Store any personal private information in a separate partition of the device, or under a separate user profile, used only for personal activities.

CONTACT Line is not legally or financially responsible if a personal device's software or hardware fails.

CONTACT Line respects the privacy of their employees and their personal devices. All precautions must be taken to keep it private and secure.

This policy allows CONTACT Line the ability to track and request access to any devices that will be used under the BYOD Policy by its employees. This access is to be used to perform required reviews and ensure the security of the device, by reviewing the compliance of the device against the requirements outlined in this policy. Employees do not have the right and should not have the expectation of privacy while using BYOD equipment subject to this Policy.

CONTACT Line - Information Security

Version #1.0.0

- Created: Mon, 05 Jul 2021 13:09:26 -0400
- Last Modified: Mon, 05 Jul 2021 14:14:06 -0400

Introduction

This policy defines:

- Information security objectives
- Roles and responsibilities
- Security guidelines and requirements for CONTACT Line information technology assets
- Security Awareness Training
- Authority & Access Control
- Data Support and Operations
- Disciplinary Actions

Information Security Objectives

Create and strengthen all internal security controls and prevent unauthorized and improper access to data by securing and ensuring the appropriate protection of information technology assets and data. All policies aim to preserve the following:

- Confidentiality - Access to data shall be confined to those with the appropriate authority.
- Integrity - Information shall be complete and accurate. All systems, assets, and networks shall operate correctly and according to specifications.
- Availability - Information shall be available and delivered to the right person when it is needed.

Roles and Responsibilities

Board of Directors

CONTACT Line has a Board of Directors who is responsible for making sure the CEO is enforcing all policies.

CEO

CONTACT Line has a CEO who is responsible for making sure the Security Officer is enforcing all policies.

Security Officer

The Security Officer is responsible for ensuring security. The Security Officer will:

- Create and manage departmental security policies
- Coordinate audits to make sure security policy is being enforced
- Coordinate CONTACT Line's incident response team
- Represent the department on the CONTACT Line Security Team
- Oversee data privacy compliance
- Communicate new or revised policies, procedures, and standards on behalf of the Security Team to all employees

Security Team

The Security Team develops, updates, and approves security policies, related procedures, and related standards. During this process, the team considers the business needs and security concerns of CONTACT Line. The team also reviews any deviation from standards/policies and then approves or denies the exceptions.

All Employees

All authorized users, staff members, employees, volunteers, and contractors who have access to CONTACT Line resources must:

- Read, understand, and follow all CONTACT Line policies
- Help protect CONTACT Line data and resources from being shared or changed without permission

Security Guidelines and Requirements

- All members of CONTACT Line must have access to the security policies, and procedures relevant to their roles and responsibilities.
- These policies, procedures, and standards must comply with and support applicable laws, regulations, and contracts.
- These policies, procedures, and standards will be reviewed no less than annually and revised as needed to reflect changes in regulatory, legal and contractual requirements.
- The Security Team must approve any exceptions to the minimum security requirements and make sure compensating controls exist.
- Any situations not specifically addressed in the policies of CONTACT Line may be identified by all employees and will be reported to Security Officer. Security Officer with help from Security Team will respond to these unique situations, learn lessons from them, and create effective policies, procedures and monitoring for them.
- All employees and those that act on behalf of CONTACT Line are required to display integrity and make ethical decisions in the execution of their relevant roles and responsibilities.
- Anyone serving as a Board of Directors will have sufficient knowledge about information security to evaluate reports addressed to them and make informed decisions.

Information Security and Privacy Awareness

To make sure all users are familiar with information security and privacy, CONTACT Line must:

- Implement training on best practices in information security and privacy policy, procedures and relevant threats to CONTACT Line. Employee security and privacy awareness training will include the secure use

of information security assets and will include the topics of Secure Authentication, Identifying Social Engineering Attacks, Sensitive Data Handling, Unintentional Data Exposure, relevant privacy regulations, Identifying and Reporting Incidents, and Breach notification requirements.
- Add information security and privacy awareness to new employee orientation materials.
- Supply CONTACT Line management with feedback on an employee's security and privacy awareness, which will be used in that employee's evaluation.

To make sure all users are familiar with security, CONTACT Line must:

- Train employees on Information Security and Privacy Awareness once a year and during employee onboarding.

Addressing Skills Gap

Skills gaps are addressed by first knowing which employees need to develop their knowledge and skills in specific areas. This can often be achieved by monitoring workforce behavioral patterns that result in incidents and data loss. Leveraging a skills gap analysis to security training strategically applies resources where they are needed most.

- Skills gaps in teams must be identified by finding out who needs additional security training.
- Skills gaps in teams must be addressed by assigning relevant training to those who need it.

Special Interest Groups

In order for CONTACT Line to implement current best practices and standards for information security, contact with special interest groups must be maintained. Contact with special interest groups can be secured by ensuring CONTACT Line is involved with any of the following:

- Obtained memberships of professional bodies
- Industry associations and events
- Participating in forums and discussion boards

Authority & Access Control

Authority and access control will be reviewed by the Security Team to ensure only the proper access is given to relevant parties. This includes access to:

- Information
- Information technology assets
- Systems
- Software
- Networks

Separation of Duties

No single individual in CONTACT Line shall have unfettered access to perform a configuration change, reproduce or decommission all data, systems or applications.

In order to ensure separation of duties is adhered to the Security Team shall be informed of any configuration change, reproduction or decommissioning of data, systems or applications via written notice.

Configuration changes, reproduction or decommissioning of data, systems or applications, must meet the approval of the Security Officer prior to the event.

In the case of emergency an emergency change, reproduction or decommissioning, the event will be recorded in an emergency change log and a written notice must be provided to the Security Officer.

Data Support and Operations

By establishing the above guidelines in the Information Security Policy and following all other associated policies, CONTACT Line incorporates security by design into its data support and operations.

Information Security in Project Management

In each project undertaking such as software development cycles and major changes in CONTACT Line business processes or technology, there exists a repeatable process for incorporating the assessment, management and consideration for security and privacy impact risks and threats into the project management process.

This process must be documented, formalized, reviewed and maintained in CONTACT Line project management procedures.

Legal and Regulatory Requirements

A record of all legal and regulatory requirements which CONTACT Line must adhered to is maintained and compliance is reviewed on a regular basis to ensure compliance with all consumer, employee rights as well as local, regional and federal laws and regulations which apply to CONTACT Line.

Disciplinary Process

There exists a defined and enforced system to correct behavior, actions, or inaction, which results in a security breach or breach of contractual obligations. A process for disciplinary and corrective measures for a breach of contractual obligations is clear and distributed to all employees.

- All Employees are required to read, understand and sign off on the policies relevant to them and prescribed to them at onboarding, annually and as their role changes.
- Employees who don't follow all policies may face disciplinary action, such as denial of access, legal penalties, and/or dismissal.
- In the case that an employee causes a data breach, the severity of disciplinary action will be determined on a case-by-case basis after a thorough investigation into the manner and intent of the breach.
- Any employee aware of a violation of these policies must report it to a supervisor or other authorized representative.
- If employees or third parties want to be exempt from any part of this policy, they must first get permission from CONTACT Line.

CONTACT Line - Password

Version #1.0.0

- Created: Mon, 05 Jul 2021 13:09:28 -0400
- Last Modified: Mon, 05 Jul 2021 14:15:17 -0400

Introduction

A strong password policy will protect CONTACT Line, your employees, and your data from external attacks. When CONTACT Line employees follow the password policy, they will make their accounts more secure: strong passwords are more difficult to steal or break.

You must follow this password policy whenever you create a work-related password or unlock code. These are some examples:

- Passwords for internal CONTACT Line resources, such as your CONTACT Line email address, any CONTACT Line account logins, and any other accounts assigned to you directly.
- Passwords for external accounts, such as vendors, clients, or other online services.
- Unlock codes for personal devices that are approved for CONTACT Line network access.

User Management

Each employee is responsible for the creation and administration of their own passwords following the guidelines of CONTACT Line Password Policy.

Use Unique Passwords or Passphrases

You must use unique passwords or passphrases for all accounts and services that you use at CONTACT Line. You must also use passwords that are different from your own personal user accounts. For instance, do not use your Facebook or Twitter passwords for any CONTACT Line accounts or services. If your Facebook or Twitter account is compromised, your corporate account has a high probability of being compromised as well.

Password Complexity Requirements

CONTACT Line passwords are created and managed by each staff member and never shared. Each password must meet the following complexity requirements:

- An 18 character or greater minimum length.
- The ability for passwords to use all special characters but no special requirement to use them.
- Do not use sequential and repetitive characters (example 1234567 or aaaaaaaaa).
- Do not use context-specific passwords, like using parts of your login username or the name of the website or service. For example, if the vendor's website is acme.com, don't create a password like ``AcmeSecret123''.
- Do not use commonly used passwords (e.g. p@ssw0rd).

- Avoid words that can be found in a dictionary, either spelled forwards or backwards, including English words, Non-English words, acronyms and proper names.
- Do not include any information that someone could easily guess based on your identity. Phone numbers, dates of birth, anniversaries, children or pet names, and home addresses should not be used in passwords.
- Use symbols and punctuation in your password. Include at least some of the following - lower case letters, upper case letters, numbers, punctuation, symbols, emojis and non-English characters.
- Passwords are never changed after the initial password set up unless they are compromised.

Default Passwords

When provisioning a new device, asset, or account, all default passwords will be changed from the default password to a password that meets CONTACT Line 'Password Complexity Requirements' in this policy.

Any passwords changed from the default string will be documented, stored and shared in an encrypted format that meets CONTACT Line 'Encryption' policy.

CONTACT Line - Remote Working

Version #1.0.0

- Created: Mon, 05 Jul 2021 13:09:26 -0400
- Last Modified: Mon, 05 Jul 2021 14:15:39 -0400

Introduction

This policy outlines how CONTACT Line protects information accessed, processed, or stored at remote working sites. These security measures help prevent issues such as theft, espionage, and sabotage. Remote working refers to all forms of work outside of the office, including nontraditional work environments such as telecommuting, flexible workplace, remote work, and virtual work environments.

The policy includes security measures for the following:

- Authorization for remote working
- Provision of remote working equipment
- Implementation of appropriate security controls
- Information security while remote working

Set up an Authorization Process for Remote Working

Only approved staff will be permitted to remote work. Staff must be authorized in writing when undertaking remote working in order to ensure security measures are in place to protect confidential information and data security.

Promote Secure Remote Working Equipment and Software

CONTACT Line must put in place measures to fully support and maintain any remote solutions.

Those responsible for managing the provisioning of remote equipment must ensure, on termination of the arrangement, the secure return or disposal of all equipment and information, in electronic and paper form, held by the employee.

Procedures relating to correct usage of any remote solution provided must be documented and explained to remote staff. In particular, the solution must support adequate data backup and remote workers must understand the backup procedure.

Any software used as part of a remote solution must be appropriately licensed.

Only CONTACT Line staff members are permitted to use CONTACT Line equipment.

Implement Appropriate Security Controls

Security controls must be implemented to mitigate risks associated with staff who access CONTACT Line's systems when remote working. The following must always be considered when approving remote requests:

- Sensitivity of information accessed or stored at the remote location
- Physical security at the remote location
- Likelihood of unauthorized access at the remote location
- Security of home wired and wireless networks
- Remote access threats

Follow the requirements for Remote Working

All staff who work remotely must follow these requirements:

Data and Encryption

- Sensitive and confidential information in electronic media cannot be stored at a remote site unless it is encrypted. You must use AES 256-bit encryption, which is the current industry-accepted level.
- Sensitive and confidential information in paper media cannot be stored at a remote site unless it is in a locked cabinet.
- Only organization-issued or approved devices can be used to process data.
- Only approved remote access methods can be used to access the organization's network.

Endpoint Hardening

- Limit access to devices to only authorized users.
- Limit and control the use of privileged utility programs or any software that requires administrative privilege to run.
- Enable auto-update on all devices for the operating system that is currently installed.
- Ensure web browsers are kept up-to-date.
- Enable auto-update on all software and applications that are installed on all devices.
- Set an inactivity timer on the device's display to turn on the screensaver or lock the screen after at least 5 minutes of inactivity.
- Ensure device requires a password on boot, waking from sleep, or after the screensaver is enabled
- When leaving your device for any period of time, lock the screen or set it to sleep.
- Ensure food and drink are consumed away from devices or in containers with a secured lid to prevent spillage.
- Disable Bluetooth connections unless required for particular devices.
- Change all default passwords when configuring any new endpoints.

Network

- Only approved remote access methods can be used to access the organization's network and resources.
- All wireless networks will enforce a WPA2 with AES 256 (WPA2-AES) encryption and are forbidden from using WPA2 with TKIP, WPA, or WEP protocols.
- All wireless network devices approved for use by CONTACT Line will have and use WPA2-AES encryption.
- All default passwords for the network will be changed as per the Password Policy.
- A separate guest network must be setup for any devices not approved as per BYOD Policy.
- All wireless devices must be audited for secure configuration to include ensuring there are no unnecessary open ports, device hardware is still supported by the manufacturer and firmware is kept up-to-date.