Version 1.1

09/03/2024

IT - Disaster Recovery Plan (DRP)

To Ensure Continuity of Operations (COOP)

Tiered Service Name

DOCUMENT OWNER:

{NAME}

{ROLE}

ANONYMOUS COMPANY, LLC

{EMAIL}

Table of Contents

1 Introduction

This Disaster Recovery Plan (DRP) captures, in a single repository, all the information that describes Anonymous Company (AnonCo) ability to withstand a disaster as well as the processes that must be followed to achieve disaster recovery.

1.1 Definition of a Disaster

An IT disaster is an unexpected event that significantly disrupts or damages an organization's IT infrastructure, systems, or services, necessitating a rapid response to minimize the impact on business operations.

- One or more mission critical systems are non-functional
- The data center(s) are not available for an extended period, but all systems are functional within it
- The data center(s) are available, but all systems are non-functional
- The data center(s) and all systems are non-functional
- An IT-Disaster has been declared by AnonCo Executive Leader

The following events can result in an IT disaster, the list is also not conclusive, as AnonCo approaches this from an all-hazards perspective. Many types of disruptions may require this Disaster Recovery and/or Business Continuity processes and accompanying policies, procedures, and plans to be activated:

- Fire
- Wildfire
- Flash flood
- Earthquake
- Pandemic
- Power Outage
- Vendor Failure
- War
- Sabotage
- Terrorism
- Hardware/Software Malfunctions
- Data Loss
- System Crashes
- Cyberattacks
  - Ransomware
  - Data Breaches
  - DDoS Attacks
  - Etc...
- Theft
- Societal Collapse
- Localized Hazards
- Regional Hazards
- Nationwide Hazards

1.2 FFIEC IT Handbook Definition of Disaster Recovery

As referenced from the FFIECT IT Handbook, section V.F.2, page 33 [11]

Disaster recovery is the restoring of IT infrastructure, data, and systems. Management should identify key business processes and activities to be maintained while IT systems and applications are unavailable and prioritize the order in which these systems are restored, which should be reflected in the BIA. In addition, management should develop a coordinated strategy for the recovery of data centers, networks, servers, storage, service monitoring, user support, and related software.

Recovery plans should address a broad range of adverse events (e.g., natural disasters, infrastructure failures, technology failures, unavailability of staff, or cyber-attacks). Disaster recovery should address guidelines for returning operations back to a normalized state with minimum disruption.

Disaster recovery should also address the following:

- Security controls and protocols, including physical and logical, for implementation and operation of recovery systems.
- Procedures for restoring backlogged activity or lost transactions to identify how transaction records will be brought current within expected recovery time frames.
- Instructions to access critical information repositories and other resources when the primary facility is unavailable.

When developing disaster recovery plans, management should exercise caution when identifying critical and non-critical systems. For example, telephone banking, internet banking, or ATMs may not seem critical when systems are operating normally; however, these systems play a critical role in delivering services to customers during a disruption. Similarly, an email system may not appear critical but may be the primary system available for communication during an adverse event. Please see FFIEC IT Handbook [11] for updated recommendations.

1.3 Data Center Recovery Alternatives

As referenced from the FFIECT IT Handbook, section V.C.1, page 29. [11]

Data center recovery alternatives vary for infrastructure, configuration, operational state, and data migration. Management should document the reasons (e.g., cost and service level) for choosing an alternative and why it is appropriate based on the entity's risk profile and complexity. The level of intervention required to activate the alternate sites affects both the cost and duration to resume operations. Recovery alternatives may take several forms, such as fully redundant systems at alternate sites, cloud-based recovery solutions (either internally developed or outsourced), another data center, or a third-party service provider. Data center and alternate site development is complex, and management should consider constraints in the analysis and design process. The primary objectives are for data to be available and remotely accessible. Management should maintain appropriate controls, regardless of solution. AnonCo leverages the below recovery site strategies:

- **Colocation Facility:** A facility that provides space, power, infrastructure, environmental controls, and telecommunications capabilities for multiple non-related tenants. If management relies on a colocation facility to deliver resources, there is a risk that the capacity at the colocation service provider may not be able to support the entity's operations during a regional or large-scale event.

- **Hot Site:** A fully operational off-site data center equipped with hardware and software used in the event of an information system disruption. Hot site development is complex, and management should consider constraints in the analysis and design process.

- **Mirrored Data Recovery Sites:** Two or more separate, active sites that back up one another with each site independently supporting critical business functions. These sites provide almost immediate resumption capacity and are seamless for end users. Physical distance and its related latency present limitations for data centers that use real-time, data mirroring backup technologies. Similar to a hot site, these sites contain all of the equipment and connectivity capabilities; however, they also have a duplicate copy of the data. This method of high availability is commonly referred to as "Active-Active."

2 Purpose

In the event of a disaster and its declaration the priority of Anonymous Company (AnonCo) is to prevent the loss of life. Before any secondary measures are undertaken, AnonCo will ensure that all employees and any individuals on the organization's premises are safe and secure.

After all individuals are deemed safe, the next goal will be to follow the steps in this DRP to restore services to business-as-usual as quickly as possible. This includes:

- Preventing the loss of the consortium's mission critical resources such as hardware, data and physical IT assets
- Minimizing downtime related to IT
- Keeping the consortium mission critical services operating in the event of a disaster

3 Scope

The Anonymous Company (AnonCo) DRP takes all the following areas into consideration:

Response Teams
(select the ones appropriate)

- Disaster Recovery
- Applications Support
- Automation
- Business Technology
- Data Center Engineering
- Data Management
- Development
- DevOps
- End User Services
- Information Security
- Networking
- Online Banking Systems
- System Administration
- Voice and Collaboration

Systems and Services
(select the ones appropriate)

- ATM Interface
- ITM Interface
- Card Wizard
- Corporate Networks
- CU Branch Networks
- CU intranet
- cView/ DNA Publisher
- DNA
    - CMC Servers
    - Core Application
    - Core Database
- DNS Hosting
- Frontier
- General Ledger
- Internet Corporate Locations
- Internet Branch Locations
- Kong/EWS for Alkami
- Loan App
- Needles
- Online Banking
- OpCon
- Openly
- Raddon Integrator Advance
- Remote Access
- Remote Deposit Capture
- Shared Branch Interface
- Temenos Akcelerant
- User Shares/ File Shares
- Velocity
- Velocity Warehouse
- Video Teller Services
- WITS

4 Activating the Disaster Recovery Plan

If a disaster occurs and is declared by the organization's executive leadership team, the priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to facilities and to reduce the impact of an IT-Disaster to the organization.

Regardless of the category that the IT-Disaster falls into, dealing with an IT-Disaster can be broken down into the following steps:

- Disaster identification and declaration
- DRP activation
- Communicating the disaster
- Assessment of current and prevention of further damage
- Hot site facility activation
- Establish IT operations
- Repair and rebuilding of primary facility

4.1 Activation Process and Considerations

To activate an IT-Disaster Recovery Plan or Process. We follow the ITILv4 process. All technological disruptions start with an Incident/ Event then that can be escalated to a Major Incident and from a MIM, we enable Disaster Recovery Activation with the Executive Leadership being the stakeholders that can activate and deactivate the IT-DR process. We need to take into consideration the complexities of declaring an IT-DR event as this will trigger cascading events and could prolong or even make the disruption worse. As part of our Critical Incident Process this would be the 5 phases to follow. Readiness, Issue Identification, Response, Recovery and Review.

Please see ***02-IT2030 AnonCo Disaster Recovery and Business Continuity Process [3], 02-IT2074 Technical Services Escalation Procedure [4], 02-IT2155 AnonCo Issue Alert Procedures [5], 02-IT2203 Incident Management Process [6], and 02-IT2204 Major Incident Process [7]*** for updated policies and procedures.

4.1.1 Business Impact Decision Process

As the incident has more impact (severity level increases) the escalation process will be invoked to involve appropriate resources. Incidents are handled at the lowest escalation level that can respond to the incident with only the resources required.

5 DRP Activation

Once the Chief Technical Officer (CTO) or alternative senior leadership at AnonCo has formally declared that a disaster has occurred they will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

- That a disaster has occurred
- The nature of the disaster (if known)
- The initial estimation of the magnitude of the disaster (if known)
- The initial estimation of the impact of the disaster (if known)
- The initial estimation of the expected duration of the disaster (if known)
- Actions that have been taken to this point
- Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads
- Scheduled meeting place for the meeting of Disaster Recovery Team Leads
- Scheduled meeting time for the meeting of Disaster Recovery Team Leads
- Any other pertinent information

If the Disaster Recovery Lead is unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Disaster Management Team Lead. Please see ***02-IT2030 AnonCo Disaster Recovery and Business Continuity Process [3], 02-IT2074 Technical Services Escalation Procedure [4]*** for updated policies and procedures.

5.1 Assessment of Current and Prevention of Further Damage

Before any employees from Anonymous Company (AnonCo) can enter the primary facility after a disaster, appropriate authorities must first ensure that the premises are safe to enter. See ***01-IT2170 Data Center Safety Policy [1].***

The first team that will be allowed to examine the primary facilities once it has been deemed safe to do so will be the Facilities Team. Once the Facilities Team has completed an examination of the building and submitted its report to the Disaster Recovery Lead, the Disaster Management, Networks, Servers, and Operations Teams will be allowed to examine the building. All teams will be required to create an initial report on the damage and provide this to the Disaster Recovery and Leadership Team within one (1) hour of the initial disaster.

During each team's review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect Anonymous Company (AnonCo)'s assets. Any necessary repairs or preventative measures must be taken to protect the facilities; these costs must first be approved by the Disaster Recovery Team Lead.

6 Data Centers

AnonCo utilizes third-party data center services provided by Flexential to ensure the reliability, security, and availability of our IT infrastructure. We have designated two primary data centers for our operations:

- **Primary Data Center:** Englewood, CO (FLEX-DEN)
  - **Location:** Englewood, Colorado
  - **Address:** 8636 S. Peoria Street, Englewood, CO 80112
  - **Provider:** Flexential
  - **Website:** https://www.flexential.com/data-centers/co/denver/englewood-data-center
  - **Role:** The Englewood data center serves as the primary data center, hosting critical applications, data, and services. It is equipped with advanced security measures, redundant power sources, and robust network connectivity to ensure continuous operations.

- **Secondary Data Center:** Collegeville, PA (FLEX-PHL)
  - **Location:** Collegeville, Pennsylvania
  - **Address:** 101 Troutman Road, Collegeville, PA 19426
  - **Provider:** Flexential
  - **Website:** https://www.flexential.com/data-centers/pa/philadelphia/collegeville-data-center
  - **Role:** The Collegeville data center functions as the secondary data center, providing backup and failover capabilities. In the event of a disruption at the primary data center, the Collegeville facility is prepared to take over operations seamlessly, minimizing downtime and ensuring business continuity.

Both data centers are strategically located to provide geographic diversity and mitigate risks associated with regional disasters. Flexential facilities are designed to meet industry standards for security, compliance, and

performance, ensuring that our IT services remain resilient and reliable. Both facilities must always have the following resources available:

- Copies of this DRP document
- Fully redundant server room and supporting services
- Sufficient servers and storage infrastructure to support enterprise business operations
- Office space for DR teams and IT to use in the event of a disaster
- External data and voice connectivity
- Sleeping quarters for employees that may need to work multiple shifts
- Kitchen facilities (including food, kitchen supplies and appliances)
- Bathroom facilities (Including toilets, showers, sinks and appropriate supplies)
- Parking spaces for employee vehicles

6.1.1 Map of Data Center – Flexential Englewood, Colorado (CO)

The nearest commercial aviation airport is Denver International Airport (DEN) and is 30 miles away from Englewood. AnonCo Headquarters is approximately 5 minutes or 2.3 miles by car from the Flexential Englewood Data Center. This has been assigned a nomenclature of FLEX-DEN in our documentation.

From Google Maps: https://maps.app.goo.gl/Yig4UNpggRW63zH9A

Flexential Englewood, CO Location

Vendor	Flexential – Denver – Englewood Data Center
Address	8636 S. Peoria Street, Englewood, CO 80112
Phone Number (General)	XXX-XXX-XXXX

Relationship Owner	Senior Director of Infrastructure Operations

6.1.2 Map of Data Center – Flexential Collegeville, Pennsylvania (PA)

The nearest commercial aviation airport is in Philadelphia (PHL) and is 24 miles away from Collegeville. From the Maryland metro area the Flexential Collegeville location is 122 miles away. From the New York metro area, the data center is 149 miles away. This has been assigned a nomenclature of FLEX-PHL in our documentation.

From Google Maps: https://maps.app.goo.gl/AHfqyAwaGiQvGGaW9

Flexential Collegeville, PA Location

Vendor	Flexential – Philadelphia – Collegeville Data Center
Address	101 Troutman Road, Collegeville, PA 19426
Phone Number (General)	XXX-XXX-XXXX
Relationship Owner	Senior Director of Infrastructure Operations

7 Data and Backups

The compilation of a comprehensive backup policy is influenced by many factors relating to the specific implementation, configuration, and availability requirements of a given application or system. System Specific Data Backup Policies and Procedures may be required to fulfill those requirements and are documented in the ***AnonCo Backup and Recovery Services Manual [2]***.

7.1 Recovery Priority based on Service Criticality

Please reference the AnonCo SLA document ***08-IT2151 Service Level Agreements [10]*** for current restoration priority.

8 Restoring IT Functionality

Should a disaster be declared, Anonymous Company (AnonCo) will exercise this plan, this section will be referred to frequently as it will contain all the information that describes the way The Consortiums' systems will be recovered.

8.1.1 Enterprise Network Diagram

8.2 Zerto Workflow and Virtual Protection Groups (VPG)

Zerto is like a superhero for banks. It helps keep important information, like customer account details and transaction records, safe. Imagine you have a big bank, and you want to make sure that no matter what happens, your bank can always stay open, and your customers' money is safe.

Zerto helps banks do that by protecting their computer data and making it easy to fix problems quickly. So, with Zerto, banks can keep running smoothly without any big interruptions, ensuring that customers can always access their money and services. In Zerto, a Virtual Protection Group (VPG) is a feature that allows you to group together virtual machines (VMs) for protection and replication purposes. Think of it as an "envelope" that contains your VMs, ensuring they are consistently protected and can be recovered together in case of a disaster.

8.2.1 Zerto Procedure

Please reference the AnonCo Procedure for *Zerto Failover, 02-IT2240 Zerto Disaster Recovery Fail Over Procedure [8]* for current process and procedures.

8.3 Cohesity Workflow

Cohesity is another superhero for banks, just like Zerto. It helps keep important information, like customer account details and transaction records, safe and secure. Imagine you have a big bank, and you want to make sure that no matter what happens, your bank can always stay open, and your customers' money is safe.

Cohesity helps banks do that by making backups of all the important data. If something bad happens, like a computer problem or a cyber-attack, Cohesity can quickly restore the data so the bank can keep running smoothly. This means customers can always access their money and services without any big interruptions.

8.3.1 Cohesity Procedure

Please reference the AnonCo Procedure for *02-IT2014 Backup and Recovery Services Manual [2]* for current process and procedures.

9 Application Playbook

This section will contain all of the information needed for the organization to get back to its regular functionality after a disaster has occurred. It is important to include all Standard Operating Procedures documents, run-books, network diagrams, software format information etc. in this section.

9.1 Revision History

The revision history shows current and previous versions of this document. Included in the comments section are descriptions of changes from previous versions.

Version	Date	Comments	Author
1.0	08/02/24	Initial Creation	Team Member 75
1.1	09/09/24	Reflow to align with AnonCo documents guidelines	Team Member 75

9.2 References

The following documents have a bearing on the activities described within the document.

List No.	Title	Document Reference No.
[1]	**01-IT2170 Data Center Safety Policy.docx**	**[1]**
[2]	**02-IT2014 Backup and Recovery Services Manual.docx**	**[2]**
[3]	**02-IT2030 AnonCo Disaster Recovery and Business Continuity Process.docx**	**[3]**
[4]	**02-IT2074 Technical Services Escalation Procedure.docx**	**[4]**
[5]	**02-IT2155 AnonCo Issue Alert Procedures.docx**	**[5]**
[6]	**02-IT2203 Incident Management Process.docx**	**[6]**
[7]	**02-IT2204 Major Incident Process.docx**	**[7]**
[8]	**02-IT2240 Zerto Disaster Recovery Fail Over Procedure.docx**	**[8]**
[9]	**02-IT2282 Cyber Incident Response Plan.docx**	**[9]**
[10]	**08-IT2151 Service Level Agreements.xlsx**	**[10]**
[11]	**FFIEC IT Handbook - https://ithandbook.ffiec.gov/**	**[11]**
[12]	**02-IT2045 AnonCo On-Call Escalation.docx**	**[12]**

9.3 Reviews and Approvals

The following table lists reviewers and approvers of this document.

	Name	Function	Date
Technical Writer	Team Member 75	Technical Writer	08/21/24
Technical Review		Subject Matter Expert	
Leadership Review	Team Member 170	Senior Director of InfraOps	

10 Appendix

10.1 Appendix A: Roles, Responsibilities and Contact Information

10.1.1 Disaster Recovery Teams & Responsibilities

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of Anonymous Company (AnonCo).

10.2 Disaster Recovery Team

The Disaster Recovery Team is responsible for overseeing and coordinating the organization's response to IT-related disasters. This team ensures that critical business functions can continue or be quickly restored in the event of a disruption. The team is comprised of organization leadership and the Business Continuity/Disaster Recovery (BC/DR) Coordinator.

10.2.1 Roles and Responsibilities

1. **Organization Leadership:**
    - **Role:** Senior executives and department heads who provide strategic direction and decision-making authority during a disaster.
    - **Responsibilities:**
        - Approve and support the disaster recovery plan.
        - Allocate resources and budget for disaster recovery efforts.
        - Communicate with stakeholders, including employees, customers, and partners.
        - Make high-level decisions regarding the prioritization of recovery efforts.
        - Ensure compliance with regulatory requirements and industry standards.
2. **BC/DR Coordinator:**
    - **Role:** The individual responsible for the development, implementation, and maintenance of the disaster recovery plan.
    - **Responsibilities:**
        - Develop and update the disaster recovery plan.
        - Coordinate disaster recovery exercises and drills.
        - Identify and assess potential risks and vulnerabilities.
        - Ensure all team members are trained and aware of their roles in the disaster recovery process.
        - Act as the primary point of contact during a disaster event.
        - Document and report on the effectiveness of the disaster recovery efforts.

10.2.2 Contact Information

Team Member 140 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX
Team Member 70 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 121 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 152 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 130 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 31 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 170 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX
Team Member 56 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 53 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 148 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 75 – w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

10.3 Applications Support Team

The Application Support Team is responsible for maintaining and supporting the organization's software applications. This team ensures that applications are running smoothly, issues are promptly addressed, and users receive the necessary support. The team is comprised of a senior leader, senior manager, and line leadership and employees.

10.3.1 Roles and Responsibilities

1. **Senior Leader:**
    - **Role:** An executive or high-level manager who provides strategic oversight and direction for the application support function.
    - **Responsibilities:**
        - Develop and communicate the vision and strategy for application support.
        - Allocate resources and budget for application support activities.
        - Ensure alignment with organizational goals and objectives.
        - Oversee major incidents and escalations.
        - Foster a culture of continuous improvement and innovation.
2. **Senior Manager:**
    - **Role:** A manager responsible for the day-to-day operations of the application support team.
    - **Responsibilities:**
        - Manage and lead the application support team.
        - Develop and implement support processes and procedures.
        - Monitor and report on team performance and application health.
        - Coordinate with other departments and stakeholders.
        - Handle escalations and ensure timely resolution of issues.
        - Provide training and development opportunities for team members.
3. **Line Leadership and Employees:**
    - **Role:** Team leads and support staff who handle the technical and operational aspects of application support.
    - **Responsibilities:**
        - Provide first and second-level support for application issues.
        - Troubleshoot and resolve application-related problems.
        - Perform routine maintenance and updates on applications.
        - Document and track support requests and resolutions.
        - Collaborate with development teams to address bugs and enhancements.
        - Ensure compliance with service level agreements (SLAs) and performance metrics.

10.3.2 Contact Information

Team Member 152 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 30 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 19 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 42 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 17 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 46 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 100 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 114 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 156 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 109 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.4 Automation Team

The Automation Team is responsible for designing, implementing, and maintaining automated processes and systems within the organization. This team aims to improve efficiency, reduce manual effort, and enhance overall productivity. The team is comprised of a senior leader, senior manager, and line employees.

10.4.1 Roles and Responsibilities

1. **Senior Leader:**
    - **Role:** An executive or high-level manager who provides strategic oversight and direction for the automation initiatives.
    - **Responsibilities:**
        - Develop and communicate the vision and strategy for automation.
        - Allocate resources and budget for automation projects.
        - Ensure alignment with organizational goals and objectives.
        - Oversee major automation initiatives and escalations.
        - Foster a culture of innovation and continuous improvement.
2. **Senior Manager:**
    - **Role:** A manager responsible for the day-to-day operations of the automation team.
    - **Responsibilities:**
        - Manage and lead the automation team.
        - Develop and implement automation processes and procedures.
        - Monitor and report on team performance and automation effectiveness.
        - Coordinate with other departments and stakeholders.
        - Handle escalations and ensure timely resolution of automation issues.
        - Provide training and development opportunities for team members.
3. **Line Employees:**
    - **Role:** Team members who handle the technical and operational aspects of automation.
    - **Responsibilities:**
        - Design, develop, and implement automated processes and systems.
        - Troubleshoot and resolve automation-related issues.
        - Perform routine maintenance and updates on automation systems.
        - Document and track automation projects and outcomes.
        - Collaborate with other teams to identify automation opportunities.
        - Ensure compliance with performance metrics and quality standards.

10.4.2 Contact Information

Team Member 152 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 30 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 188 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 95 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 15 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 36 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 23 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.5 Business Technology Team

The Business Technology Team is responsible for managing and supporting the technology infrastructure and systems that enable business operations. This team ensures that technology solutions align with business needs and drive efficiency and innovation. The team is comprised of a senior leader, a manager, and line employees.

10.5.1 Roles and Responsibilities

1. **Senior Leader:**
    - **Role:** An executive or high-level manager who provides strategic oversight and direction for business technology initiatives.
    - **Responsibilities:**
        - Develop and communicate the vision and strategy for business technology.
        - Allocate resources and budget for technology projects.
        - Ensure alignment with organizational goals and objectives.
        - Oversee major technology initiatives and escalations.
        - Foster a culture of innovation and continuous improvement.
2. **Manager:**
    - **Role:** A manager responsible for the day-to-day operations of the business technology team.
    - **Responsibilities:**
        - Manage and lead the business technology team.
        - Develop and implement technology processes and procedures.
        - Monitor and report on team performance and technology effectiveness.
        - Coordinate with other departments and stakeholders.
        - Handle escalations and ensure timely resolution of technology issues.
        - Provide training and development opportunities for team members.
3. **Line Employees:**
    - **Role:** Team members who handle the technical and operational aspects of business technology.
    - **Responsibilities:**
        - Implement and support technology solutions that meet business needs.
        - Troubleshoot and resolve technology-related issues.
        - Perform routine maintenance and updates on technology systems.
        - Document and track technology projects and outcomes.
        - Collaborate with other teams to identify technology opportunities.
        - Ensure compliance with performance metrics and quality standards.

10.5.2 Contact Information

Team Member 152 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 101 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 119 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 08 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 122 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 168 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 09 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 47 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.6 Data Center Engineering Team

The Data Center Engineering Team is responsible for the design, implementation, and maintenance of the organization's data center infrastructure. This team ensures that data centers operate efficiently, securely, and reliably to support business operations. The team is comprised of a director, a senior manager, and line employees.

10.6.1 Roles and Responsibilities

1. **Director:**
    - **Role:** An executive or high-level manager who provides strategic oversight and direction for data center operations.
    - **Responsibilities:**
        - Develop and communicate the vision and strategy for data center engineering.
        - Allocate resources and budget for data center projects.
        - Ensure alignment with organizational goals and objectives.
        - Oversee major data center initiatives and escalations.
        - Foster a culture of innovation and continuous improvement.
2. **Senior Manager:**
    - **Role:** A manager responsible for the day-to-day operations of the data center engineering team.
    - **Responsibilities:**
        - Manage and lead the data center engineering team.
        - Develop and implement data center processes and procedures.
        - Monitor and report on team performance and data center health.
        - Coordinate with other departments and stakeholders.
        - Handle escalations and ensure timely resolution of data center issues.
        - Provide training and development opportunities for team members.
3. **Line Employees:**
    - **Role:** Team members who handle the technical and operational aspects of data center engineering.
    - **Responsibilities:**
        - Design, develop, and implement data center infrastructure.
        - Troubleshoot and resolve data center-related issues.
        - Perform routine maintenance and updates on data center systems.
        - Document and track data center projects and outcomes.
        - Collaborate with other teams to ensure data center reliability and efficiency.
        - Ensure compliance with performance metrics and quality standards.

10.6.2 Contact Information

Team Member 130 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 137 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 116 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 185 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 52 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 13 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 131 - w XXX-XXX-XXXX

10.7 Data Management Team

The Data Management Team is responsible for overseeing and maintaining the organization's databases. This includes ensuring data integrity, availability, and security, as well as supporting disaster recovery efforts.

10.7.1 Roles and Responsibilities

1. **Manager:**
    - **Role:** Oversees the entire Data Management Team and ensures alignment with organizational goals.
    - **Responsibilities:**
        - Develop and implement data management policies and procedures.
        - Coordinate disaster recovery planning and execution.
        - Ensure compliance with relevant regulations and standards.
        - Manage team performance and provide guidance and support.
        - Liaise with other departments to ensure data needs are met.
2. **Database Admin Lead:**
    - **Role:** Leads the database administration efforts and acts as the primary technical expert.
    - **Responsibilities:**
        - Design, implement, and maintain database systems.
        - Monitor database performance and optimize as needed.
        - Ensure data backups and recovery processes are in place and tested.
        - Troubleshoot and resolve database issues.
        - Provide technical support and training to line employees.
3. **Line Employees:**
    - **Role:** Support the day-to-day operations of the Data Management Team.
    - **Responsibilities:**
        - Perform routine database maintenance tasks.
        - Assist in data backup and recovery processes.
        - Monitor database systems and report issues to the Database Admin Lead.
        - Ensure data integrity and security.
        - Participate in disaster recovery drills and exercises.

10.7.2 Contact Information

Team Member 89 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 94 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 182 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 153 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 35 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 113 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 157 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 147 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.8 Development Team

The Development Team is responsible for designing, coding, testing, and maintaining software applications. This team ensures that software solutions meet the organization's needs and are delivered on time and within budget.

10.8.1 Roles and Responsibilities

1. **Senior Leader:**
    - **Role:** Provides strategic direction and oversight for the entire Development Team.
    - **Responsibilities:**
        - Define the overall software development strategy and vision.
        - Ensure alignment with organizational goals and objectives.
        - Oversee major projects and initiatives.
        - Foster a culture of innovation and continuous improvement.
        - Liaise with other senior leaders to ensure cross-functional collaboration.
2. **Senior Manager:**
    - **Role:** Manages the day-to-day operations of the Development Team and ensures project delivery.
    - **Responsibilities:**
        - Develop and implement project plans and timelines.
        - Allocate resources and manage team workload.
        - Monitor project progress and address any issues or roadblocks.
        - Ensure adherence to development standards and best practices.
        - Provide mentorship and support to managers and team members.
3. **Manager:**
    - **Role:** Oversees specific projects or sub-teams within the Development Team.
    - **Responsibilities:**
        - Coordinate project activities and ensure timely delivery.
        - Manage team performance and provide feedback.
        - Collaborate with other managers and stakeholders.
        - Ensure quality and consistency in code and documentation.
        - Support the professional development of team members.
4. **Software QA Leader:**
    - **Role:** Leads the quality assurance efforts to ensure software reliability and performance.
    - **Responsibilities:**
        - Develop and implement QA processes and standards.
        - Plan and execute testing strategies and test cases.
        - Identify and report defects and issues.
        - Collaborate with developers to ensure timely resolution of issues.
        - Provide training and support to QA team members.
5. **Line Employees:**
    - **Role:** Execute the day-to-day tasks related to software development and quality assurance.
    - **Responsibilities:**
        - Write, test, and maintain code.
        - Participate in code reviews and provide feedback.
        - Perform unit and integration testing.
        - Document code and development processes.
        - Collaborate with team members to resolve issues and improve software quality.

10.8.2 Contact Information

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX
- Team Member 51 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 167 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 124 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 146 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 34 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 03 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 192 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 102 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 10 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 81 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 187 - w XXX-XXX-XXXX c XXX-XXX-XXXX
    - Team Member 190 - w XXX-XXX-XXXX
  - Team Member 24 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 61 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 120 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 01 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 171 - w XXX-XXX-XXXX c XXX-XXX-XXXX
  - Team Member 65 - w XXX-XXX-XXXX

10.9 DevOps Team

The DevOps team is responsible for bridging the gap between development and operations, ensuring seamless integration, continuous delivery, and high availability of systems. This team plays a crucial role in maintaining the stability and scalability of IT infrastructure.

10.9.1 Roles and Responsibilities

1. Senior Leader
   - **Role**: Oversees the entire DevOps team and ensures alignment with organizational goals.
   - **Responsibilities**:
     - Develop and communicate the strategic vision for DevOps.
     - Ensure resources are allocated effectively.
     - Liaise with other senior leaders to integrate DevOps practices across the organization.
     - Monitor and evaluate the performance of the DevOps team.
2. Director
   - **Role**: Manages the overall operations of the DevOps team and ensures the implementation of best practices.
   - **Responsibilities**:
     - Develop and enforce DevOps policies and procedures.
     - Coordinate with other departments to ensure seamless integration of DevOps practices.
     - Oversee the implementation of disaster recovery plans.
     - Ensure compliance with industry standards and regulations.
3. Manager
   - **Role**: Supervises day-to-day activities of the DevOps team and ensures project milestones are met.
   - **Responsibilities**:
     - Assign tasks and monitor progress.
     - Provide guidance and support to team members.
     - Ensure timely and effective communication within the team.
     - Identify and mitigate risks related to DevOps operations.
4. Lead Engineer
   - **Role**: Leads the technical aspects of DevOps projects and ensures the reliability and scalability of systems.
   - **Responsibilities**:
     - Design and implement infrastructure and automation solutions.
     - Troubleshoot and resolve technical issues.
     - Mentor junior engineers and provide technical guidance.
     - Collaborate with other teams to ensure system integration and performance.
5. Line Employees
   - **Role**: Execute day-to-day DevOps tasks and support the implementation of disaster recovery plans.
   - **Responsibilities**:
     - Perform routine maintenance and monitoring of systems.
     - Implement automation scripts and tools.
     - Participate in incident response and resolution.
     - Document processes and procedures for future reference.

10.9.2 Contact Information

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 170 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX
Team Member 178 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 37 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 134 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 82 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 05 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.10 End User Services Team

The Desktop Support team provides on-site technical support to end users, ensuring the smooth operation of desktop systems and peripherals. This team is distributed across multiple locations to provide localized support.

10.10.1 Roles and Responsibilities

1. **Senior Leader**
    - **Role**: Oversees the Desktop Support team and ensures alignment with organizational goals.
    - **Responsibilities**:
        - Develop and communicate the strategic vision for Desktop Support.
        - Ensure resources are allocated effectively.
        - Liaise with other senior leaders to integrate Desktop Support practices across the organization.
        - Monitor and evaluate the performance of the Desktop Support team.
2. **Senior Manager**
    - **Role**: Manages the overall operations of the Desktop Support team.
    - **Responsibilities**:
        - Develop and enforce Desktop Support policies and procedures.
        - Coordinate with other departments to ensure seamless integration of Desktop Support practices.
        - Oversee the implementation of disaster recovery plans.
        - Ensure compliance with industry standards and regulations.
3. **Manager (New York)**
    - **Role**: Supervises day-to-day activities of the Desktop Support team in New York.
    - **Responsibilities**:
        - Assign tasks and monitor progress.
        - Provide guidance and support to team members.
        - Ensure timely and effective communication within the team.
        - Identify and mitigate risks related to Desktop Support operations.
4. **Lead (New York)**
    - **Role**: Leads the technical aspects of Desktop Support operations in New York.
    - **Responsibilities**:
        - Design and implement support solutions.
        - Troubleshoot and resolve technical issues.
        - Mentor junior staff and provide technical guidance.
        - Collaborate with other teams to ensure system integration and performance.
5. **Line Employees (New York)**
    - **Role**: Execute day-to-day Desktop Support tasks in New York.
    - **Responsibilities**:
        - Perform routine maintenance and monitoring of systems.
        - Implement support scripts and tools.
        - Participate in incident response and resolution.
        - Document processes and procedures for future reference.
6. **Manager (Colorado)**
    - **Role**: Supervises day-to-day activities of the Desktop Support team in Colorado.
    - **Responsibilities**:
        - Assign tasks and monitor progress.
        - Provide guidance and support to team members.

        - Ensure timely and effective communication within the team.
        - Identify and mitigate risks related to Desktop Support operations.
7. **Lead (Colorado)**
    - **Role**: Leads the technical aspects of Desktop Support operations in Colorado.
    - **Responsibilities**:
        - Design and implement support solutions.
        - Troubleshoot and resolve technical issues.
        - Mentor junior staff and provide technical guidance.
        - Collaborate with other teams to ensure system integration and performance.
8. **Line Employees (Colorado)**
    - **Role**: Execute day-to-day Desktop Support tasks in Colorado.
    - **Responsibilities**:
        - Perform routine maintenance and monitoring of systems.
        - Implement support scripts and tools.
        - Participate in incident response and resolution.
        - Document processes and procedures for future reference.
9. **Manager (Maryland)**
    - **Role**: Supervises day-to-day activities of the Desktop Support team in Maryland.
    - **Responsibilities**:
        - Assign tasks and monitor progress.
        - Provide guidance and support to team members.
        - Ensure timely and effective communication within the team.
        - Identify and mitigate risks related to Desktop Support operations.
10. **Lead (Maryland)**
    - **Role**: Leads the technical aspects of Desktop Support operations in Maryland.
    - **Responsibilities**:
        - Design and implement support solutions.
        - Troubleshoot and resolve technical issues.
        - Mentor junior staff and provide technical guidance.
        - Collaborate with other teams to ensure system integration and performance.
11. **Line Employees (Maryland)**
    - **Role**: Execute day-to-day Desktop Support tasks in Maryland.
    - **Responsibilities**:
        - Perform routine maintenance and monitoring of systems.
        - Implement support scripts and tools.
        - Participate in incident response and resolution.
        - Document processes and procedures for future reference.

10.10.2 Contact Information

Service Desk

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 184 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 38 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 104 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 93 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 160 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 166 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 12 - w XXX-XXX-XXXX

Team Member 133 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 44 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 103 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 04 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 20 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 96 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 136 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Deskside

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 184 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 33 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 123 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 129 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 66 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 76 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 63 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 69 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 118 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 18 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 107 - w XXX-XXX-XXXX
Team Member 16 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 143 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 45 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 29 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 64 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 07 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 87 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 43 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 99 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 126 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Account Provisioning

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 184 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 161 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 169 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 67 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 164 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 186 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 74 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 39 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 32 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 90 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.11 Information Security Team

The Information Security team is responsible for protecting the organization's information assets from cyber threats and ensuring compliance with security policies and regulations. This team plays a critical role in maintaining the confidentiality, integrity, and availability of data.

10.11.1 Roles and Responsibilities

1. Senior Leader
   - **Role**: Oversees the Information Security team and ensures alignment with organizational goals.
   - **Responsibilities**:
     - Develop and communicate the strategic vision for information security.
     - Ensure resources are allocated effectively.
     - Liaise with other senior leaders to integrate security practices across the organization.
     - Monitor and evaluate the performance of the Information Security team.
2. Senior Manager
   - **Role**: Manages the overall operations of the Information Security team.
   - **Responsibilities**:
     - Develop and enforce information security policies and procedures.
     - Coordinate with other departments to ensure seamless integration of security practices.
     - Oversee the implementation of disaster recovery plans.
     - Ensure compliance with industry standards and regulations.
3. Manager
   - **Role**: Supervises day-to-day activities of the Information Security team.
   - **Responsibilities**:
     - Assign tasks and monitor progress.
     - Provide guidance and support to team members.
     - Ensure timely and effective communication within the team.
     - Identify and mitigate risks related to information security operations.
4. Principal Security Architect
   - **Role**: Leads the technical aspects of information security and ensures the design and implementation of robust security solutions.
   - **Responsibilities**:
     - Design and implement security architecture and frameworks.
     - Conduct security assessments and vulnerability analyses.
     - Develop and maintain security standards and best practices.
     - Collaborate with other teams to ensure secure system integration and performance.
5. Line Employees
   - **Role**: Execute day-to-day information security tasks and support the implementation of security measures.
   - **Responsibilities**:
     - Perform routine security monitoring and incident response.
     - Implement security tools and technologies.
     - Participate in security awareness and training programs.
     - Document security processes and procedures for future reference.

10.11.2 Contact Information

Team Member 56 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 181 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 40 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 86 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 135 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 50 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 02 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 57 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 117 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 138 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 26 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 53 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 41 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 174 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 60 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.12 Network Team

The Network Team is responsible for designing, implementing, and maintaining the organization's network infrastructure. This team ensures the reliability, security, and performance of network operations.

10.12.1 Roles and Responsibilities

1. Senior Leader
   - **Role**: Oversees the entire Network Team and ensures alignment with organizational goals.
   - **Responsibilities**:
     - Develop and communicate strategic vision for network operations.
     - Ensure resources are allocated effectively.
     - Liaise with other senior leaders to integrate network practices across the organization.
     - Monitor and evaluate the performance of the Network Team.
2. Director
   - **Role**: Manages the overall operations of the Network Team and ensures the implementation of best practices.
   - **Responsibilities**:
     - Develop and enforce network policies and procedures.
     - Coordinate with other departments to ensure seamless integration of network practices.
     - Oversee the implementation of disaster recovery plans.
     - Ensure compliance with industry standards and regulations.
3. Senior Manager
   - **Role**: Manages the day-to-day operations of the Network Team.
   - **Responsibilities**:
     - Assign tasks and monitor progress.
     - Provide guidance and support to team members.
     - Ensure timely and effective communication within the team.
     - Identify and mitigate risks related to network operations.
4. Manager of Network Operations
   - **Role**: Oversees the network operations and ensures the reliability and performance of the network infrastructure.
   - **Responsibilities**:
     - Monitor network performance and troubleshoot issues.
     - Implement network upgrades and improvements.
     - Coordinate with other teams to ensure network integration and performance.
     - Develop and maintain network documentation and procedures.
5. Manager of Firewall Operations
   - **Role**: Manages the firewall operations and ensures the security of the network infrastructure.
   - **Responsibilities**:
     - Implement and manage firewall policies and configurations.
     - Monitor firewall performance and troubleshoot issues.
     - Conduct security assessments and vulnerability analyses.
     - Collaborate with the Information Security team to ensure network security.
6. Network Architect
   - **Role**: Leads the design and implementation of network architecture and solutions.
   - **Responsibilities**:
     - Design and implement network infrastructure and solutions.

- Conduct network assessments and performance analyses.
- Develop and maintain network standards and best practices.
- Collaborate with other teams to ensure network integration and performance.

7. Line Engineers
   - **Role**: Execute day-to-day network tasks and support the implementation of network solutions.
   - **Responsibilities**:
     - Perform routine network maintenance and monitoring.
     - Implement network configurations and upgrades.
     - Participate in incident response and resolution.
     - Document network processes and procedures for future reference.

10.12.2 Contact Information

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 130 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 132 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 142 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 21 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 55 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 71 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 139 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 191 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 22 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 62 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 149 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 49 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 92 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.13 Online Banking Systems Team

The Online Banking Systems team is responsible for the development, maintenance, and support of the organization's online banking platforms. This team ensures that the online banking systems are secure, reliable, and user-friendly, providing customers with seamless access to banking services. The team collaborates with other departments to integrate online banking with other business functions and ensures compliance with regulatory requirements.

10.13.1 Roles and Responsibilities

1. Director
   - **Role**: Oversees the entire Online Banking Systems team and ensures alignment with organizational goals and strategies.
   - **Responsibilities**:
     - Develop and implement strategic plans for online banking systems.
     - Ensure compliance with regulatory requirements and industry standards.
     - Coordinate with other departments to integrate online banking systems with other business functions.
     - Manage budget and resource allocation for the team.
     - Provide leadership and guidance to the team.
2. Senior Manager
   - **Role**: Manages the day-to-day operations of the online banking systems and supports the Director in strategic planning.
   - **Responsibilities**:
     - Oversee the implementation and maintenance of online banking systems.
     - Ensure system availability, performance, and security.
     - Coordinate with vendors and service providers.
     - Develop and enforce policies and procedures for system use and security.
     - Mentor and support managers and line employees.
3. Manager
   - **Role**: Supervises specific aspects of the online banking systems and ensures smooth operation.
   - **Responsibilities**:
     - Manage the development and deployment of new features and updates.
     - Monitor system performance and troubleshoot issues.
     - Ensure data integrity and security.
     - Coordinate with other teams for system integration and support.
     - Provide training and support to line employees.
4. Line Employees
   - **Role**: Execute day-to-day tasks and support the operation and maintenance of online banking systems.
   - **Responsibilities**:
     - Perform routine system checks and maintenance.
     - Assist in the development and testing of new features.
     - Respond to user inquiries and issues.
     - Ensure data accuracy and security.
     - Document processes and procedures.

10.13.2 Contact Information

Team Member 152 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 30 - w XXX-XXX-XXXX h XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 98 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 111 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 173 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 84 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 85 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.14 Strategic Planning (PMO) Team

The Strategic Planning (PMO) team is responsible for overseeing the planning, execution, and completion of strategic projects within the organization. This team ensures that projects align with the company's goals and objectives, are delivered on time, and within budget. The team collaborates with various departments to ensure successful project outcomes and continuous improvement.

10.14.1 Roles and Responsibilities

1. Senior Director
   - **Role**: Leads the Strategic Planning (PMO) team and ensures alignment with organizational strategies and goals.
   - **Responsibilities**:
     - Develop and implement strategic project management frameworks and methodologies.
     - Oversee the portfolio of strategic projects and ensure alignment with business objectives.
     - Manage budget and resource allocation for the PMO.
     - Provide leadership and guidance to the team.
     - Ensure compliance with regulatory requirements and industry standards.
2. Senior Manager
   - **Role**: Manages the day-to-day operations of the PMO and supports the Senior Director in strategic planning.
   - **Responsibilities**:
     - Oversee the execution and delivery of strategic projects.
     - Ensure project management best practices are followed.
     - Coordinate with project managers and other stakeholders.
     - Develop and enforce policies and procedures for project management.
     - Mentor and support project managers and other team members.
3. Head of Product Ownership
   - **Role**: Leads the product ownership function within the PMO and ensures alignment with business goals.
   - **Responsibilities**:
     - Define and prioritize product features and requirements.
     - Collaborate with stakeholders to ensure product alignment with business objectives.
     - Oversee the development and delivery of product roadmaps.
     - Ensure effective communication between product owners and project teams.
     - Provide guidance and support to product owners.
4. Project Managers
   - **Role**: Manage specific projects within the PMO and ensure successful delivery.
   - **Responsibilities**:
     - Plan, execute, and close projects according to defined timelines and budgets.
     - Coordinate with stakeholders to define project scope and objectives.
     - Monitor project progress and address any issues or risks.
     - Ensure effective communication and collaboration among project team members.
     - Document project processes and outcomes.

10.14.2 Contact Information

Team Member 121 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 25 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 48 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 189 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 127 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 158 - w XXX-XXX-XXXX
Team Member 54 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 125 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 14 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 83 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 176 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 172 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 150 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 179 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.15 System Administration Team

The System Administration team is responsible for the installation, configuration, maintenance, and reliable operation of the organization's IT infrastructure. This team ensures that systems are running smoothly and efficiently, provides technical support, and implements security measures to protect the organization's data and systems. The team collaborates with other departments to support business operations and strategic initiatives.

10.15.1 Roles and Responsibilities

1. Senior Leader
   - **Role**: Provides overall leadership and strategic direction for the System Administration team.
   - **Responsibilities**:
     - Develop and implement strategic plans for IT infrastructure.
     - Ensure alignment with organizational goals and objectives.
     - Oversee budget and resource allocation for the team.
     - Provide leadership and guidance to the team.
     - Ensure compliance with regulatory requirements and industry standards.
2. Director
   - **Role**: Manages the System Administration team and supports the Senior Leader in strategic planning.
   - **Responsibilities**:
     - Oversee the implementation and maintenance of IT systems.
     - Ensure system availability, performance, and security.
     - Coordinate with other departments and stakeholders.
     - Develop and enforce policies and procedures for system administration.
     - Mentor and support senior managers and other team members.
3. Senior Manager
   - **Role**: Manages the day-to-day operations of the System Administration team.
   - **Responsibilities**:
     - Oversee system administration tasks and projects.
     - Ensure system performance and reliability.
     - Coordinate with vendors and service providers.
     - Develop and enforce policies and procedures for system use and security.
     - Mentor and support managers and other team members.
4. Manager
   - **Role**: Supervises specific aspects of system administration and ensures smooth operation.
   - **Responsibilities**:
     - Manage the deployment and maintenance of IT systems.
     - Monitor system performance and troubleshoot issues.
     - Ensure data integrity and security.
     - Coordinate with other teams for system integration and support.
     - Provide training and support to line employees.
5. Lead
   - **Role**: Provides technical leadership and expertise within the System Administration team.
   - **Responsibilities**:
     - Lead the implementation of complex system administration tasks.
     - Provide technical guidance and support to team members.
     - Ensure adherence to best practices and standards.
     - Collaborate with other teams on technical projects.

- Mentor and support junior team members.

6. Enterprise Architect
   - **Role**: Designs and oversees the implementation of the organization's IT infrastructure.
   - **Responsibilities**:
     - Develop and maintain the enterprise architecture framework.
     - Ensure alignment with business goals and objectives.
     - Collaborate with stakeholders to define IT infrastructure requirements.
     - Oversee the integration of new technologies and systems.
     - Provide guidance and support to system architects and administrators.
7. System Architect
   - **Role**: Designs and implements specific IT systems within the organization's infrastructure.
   - **Responsibilities**:
     - Develop and maintain system architecture designs.
     - Ensure system alignment with business requirements.
     - Collaborate with stakeholders to define system requirements.
     - Oversee the implementation and integration of IT systems.
     - Provide technical guidance and support to system administrators.
8. Senior System and Storage Administrator
   - **Role**: Manages the organization's storage systems and ensures data availability and security.
   - **Responsibilities**:
     - Oversee the implementation and maintenance of storage systems.
     - Ensure data integrity and security.
     - Monitor storage system performance and troubleshoot issues.
     - Develop and enforce policies and procedures for data storage.
     - Provide technical guidance and support to system administrators.
9. System Administrators
   - **Role**: Execute day-to-day tasks and support the operation and maintenance of IT systems.
   - **Responsibilities**:
     - Perform routine system checks and maintenance.
     - Assist in the development and testing of new systems.
     - Respond to user inquiries and issues.
     - Ensure data accuracy and security.
     - Document processes and procedures.

10.15.2 Contact Information

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 170 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 177 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 110 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 180 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 58 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 88 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 27 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 144 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 78 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 183 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 72 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 115 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 97 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 155 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 154 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 128 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 80 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 28 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 162 - w XXX-XXX-XXXX c XXX-XXX-XXXX
Team Member 06 - w XXX-XXX-XXXX c XXX-XXX-XXXX

10.16 Voice and Collaboration Team

The Voice and Collaboration team is responsible for the design, implementation, and maintenance of the organization's voice and collaboration systems. This team ensures that communication and collaboration tools are reliable, secure, and efficient, enabling seamless interaction among employees and with external stakeholders. The team collaborates with other departments to support business operations and strategic initiatives.

10.16.1 Roles and Responsibilities

1. Senior Leader
   - **Role**: Provides overall leadership and strategic direction for the Voice and Collaboration team.
   - **Responsibilities**:
     - Develop and implement strategic plans for voice and collaboration systems.
     - Ensure alignment with organizational goals and objectives.
     - Oversee budget and resource allocation for the team.
     - Provide leadership and guidance to the team.
     - Ensure compliance with regulatory requirements and industry standards.
2. Director
   - **Role**: Manages the Voice and Collaboration team and supports the Senior Leader in strategic planning.
   - **Responsibilities**:
     - Oversee the implementation and maintenance of voice and collaboration systems.
     - Ensure system availability, performance, and security.
     - Coordinate with other departments and stakeholders.
     - Develop and enforce policies and procedures for system use and security.
     - Mentor and support the voice architect, lead, and engineers.
3. Voice Architect
   - **Role**: Designs and oversees the implementation of the organization's voice communication systems.
   - **Responsibilities**:
     - Develop and maintain the voice architecture framework.
     - Ensure alignment with business goals and objectives.
     - Collaborate with stakeholders to define voice communication requirements.
     - Oversee the integration of new voice technologies and systems.
     - Provide guidance and support to the lead and engineers.
4. Lead
   - **Role**: Provides technical leadership and expertise within the Voice and Collaboration team.
   - **Responsibilities**:
     - Lead the implementation of complex voice and collaboration tasks.
     - Provide technical guidance and support to team members.
     - Ensure adherence to best practices and standards.
     - Collaborate with other teams on technical projects.
     - Mentor and support junior team members.
5. Engineers
   - **Role**: Execute day-to-day tasks and support the operation and maintenance of voice and collaboration systems.
   - **Responsibilities**:
     - Perform routine system checks and maintenance.
     - Assist in the development and testing of new voice and collaboration systems.

- Respond to user inquiries and issues.
- Ensure data accuracy and security.
- Document processes and procedures.

10.16.2 Contact Information

Team Member 165 - w XXX-XXX-XXXX c XXX-XXX-XXXX

Team Member 31 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 77 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 175 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 151 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 159 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 91 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

Team Member 145 - w XXX-XXX-XXXX c XXX-XXX-XXXX other XXX-XXX-XXXX

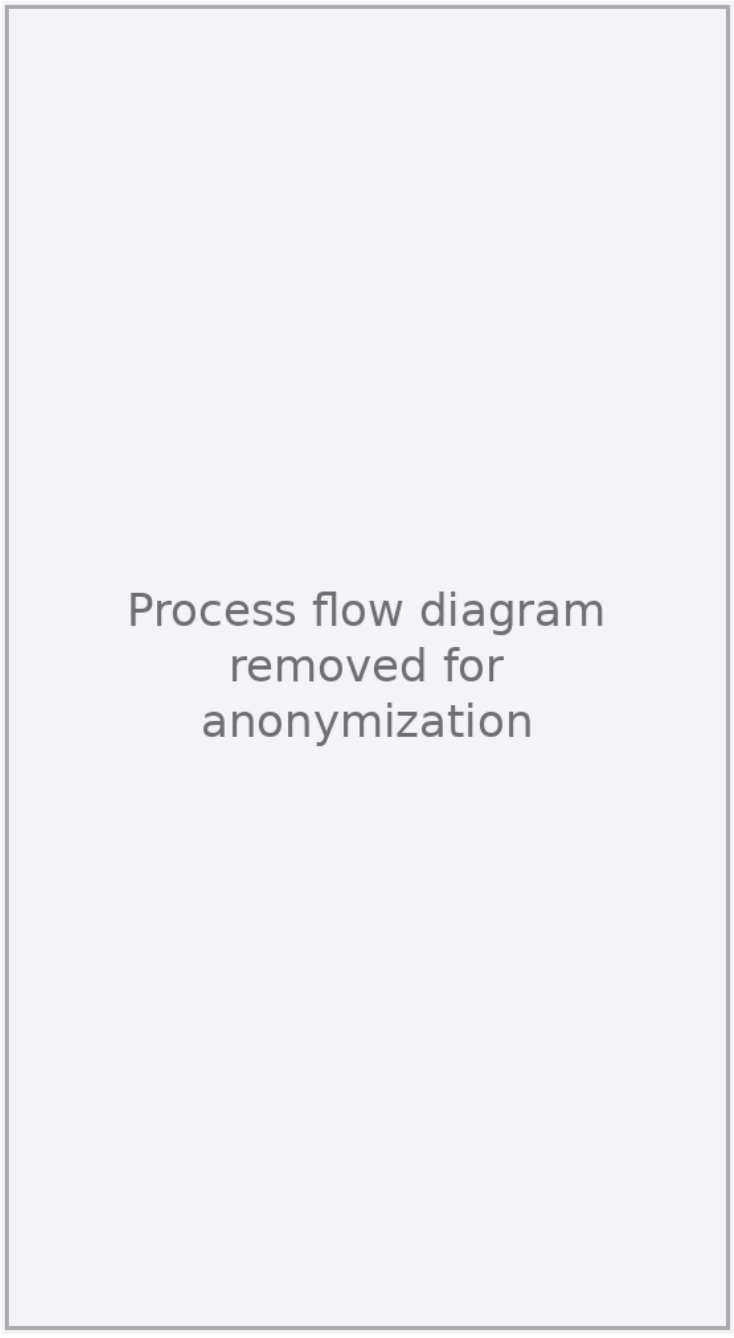
11 Appendix B: Partner Contacts

Business/Segment	Contact Level	Contact Name	Phone Numbers
Credit Union Alpha	Technical	Team Member 11	Office: XXX-XXX-XXXX Mobile: XXX-XXX-XXXX
Credit Union Alpha	Executive	Team Member 68	Office: XXX-XXX-XXXX Mobile: XXX-XXX-XXXX
Credit Union Alpha	Technical	Team Member 59	Office: XXX-XXX-XXXX Mobile: XXX-XXX-XXXX
Credit Union Bravo	Executive	Team Member 163	Phone: XXX-XXX-XXXX
Credit Union Bravo	Executive	Team Member 141	Office: XXX-XXX-XXXX
Credit Union Bravo	Executive	Team Member 112	Mobile: XXX-XXX-XXXX
Credit Union Charlie	Executive	Team Member 105	Office: XXX-XXX-XXXX Mobile: XXX-XXX-XXXX
Credit Union Charlie	Executive	Team Member 73	Mobile: XXX-XXX-XXXX
Shared Services Org	Executive	Team Member 108	Office: XXX-XXX-XXXX Mobile: XXX-XXX-XXXX
Shared Services Org	Executive	Team Member 79	Mobile: XXX-XXX-XXXX
Shared Services Org	Executive	Team Member 106	Office: XXX-XXX-XXXX Mobile: XXX-XXX-XXXX

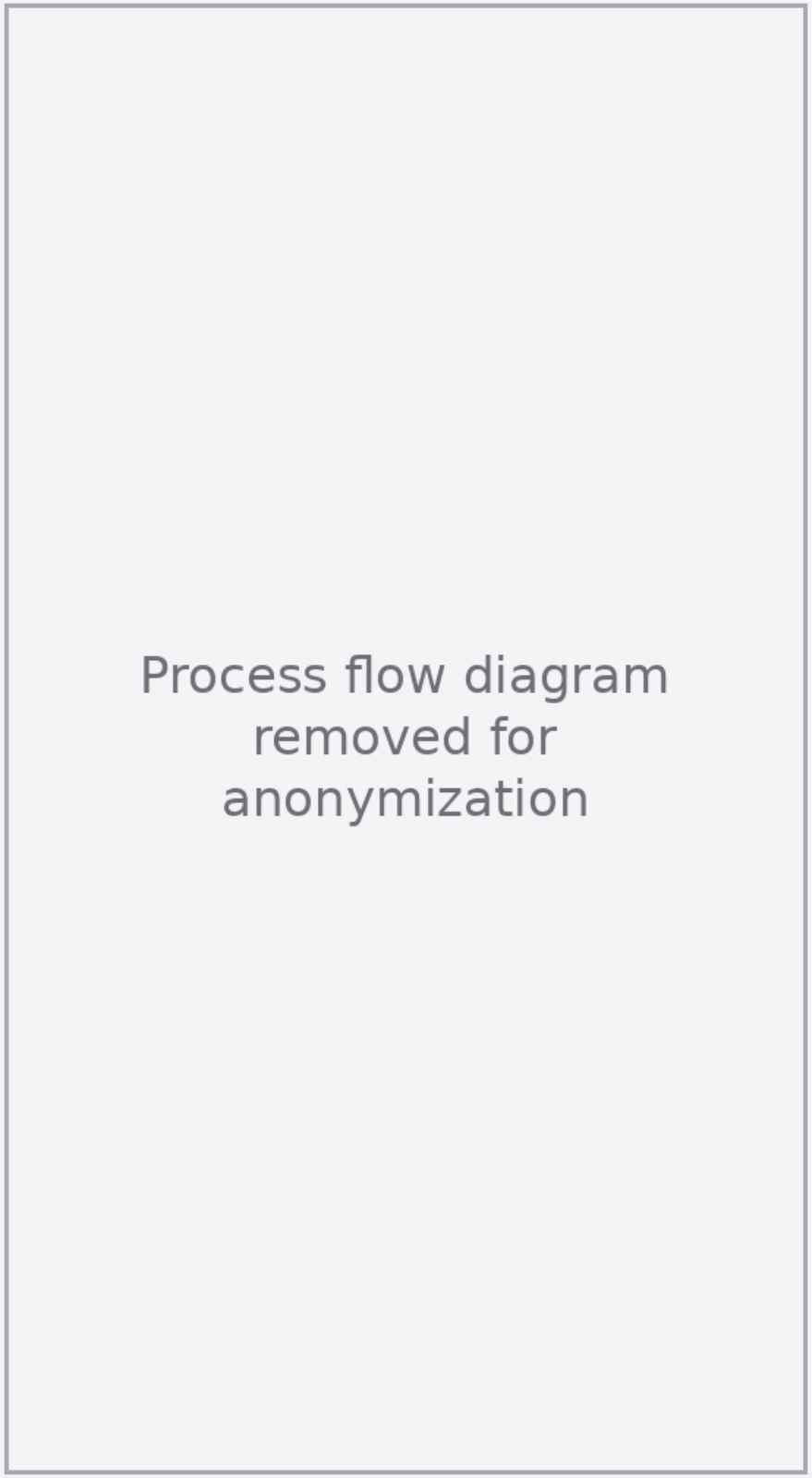
12 Appendix C: Process Flows

12.1 AnonCo Incident Management Process Flow

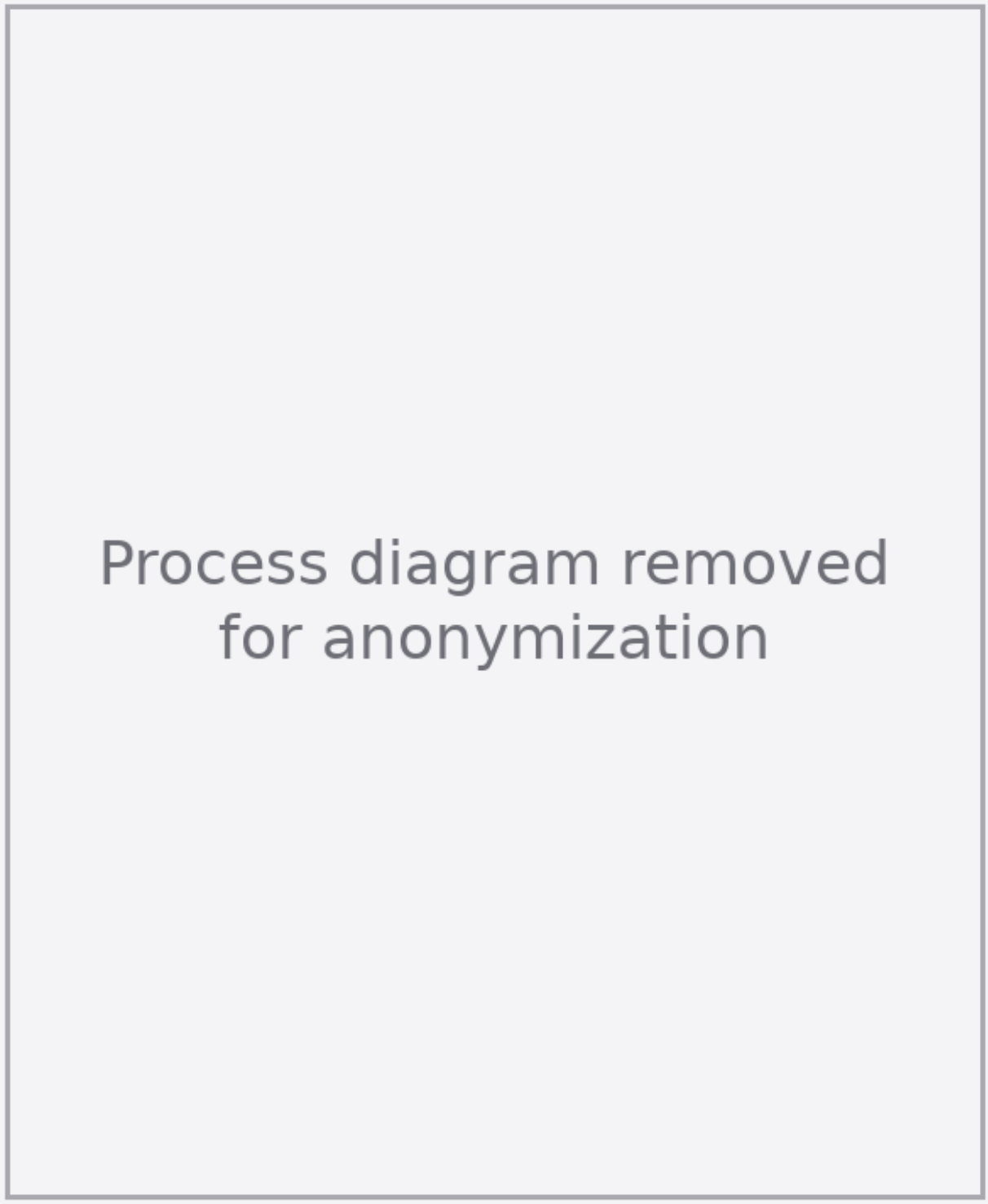
When identifying an incident/ event and the resulting escalation, time is of the essence. Understanding decisions and points of escalation are critical. Decision points are also communication points as pivots and escalation decisions may or may not impact how our consortium partners operate and recover from adversity. Below is the process flow from event/ incident escalated to Major/Critical Incident with recovery and post-mortem actions.



12.2 AnonCo Critical/ Major Incident Management Process Flow

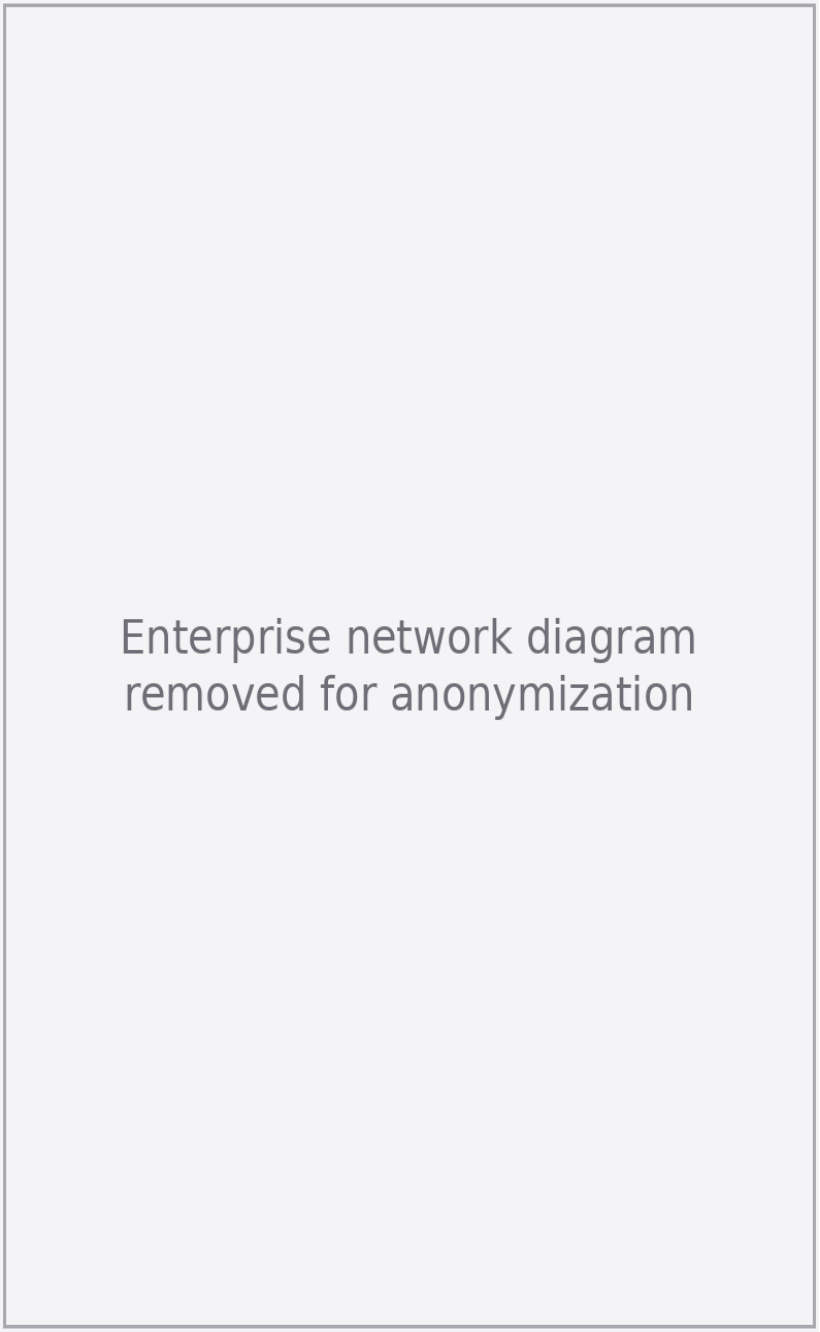


12.3 Troubleshooting and Triage Process Flow



12.4 P1 Incident to DR Declaration Process Flow

In a disaster recovery or business continuity emergency, time is of the essence. Understanding decisions and points of escalation are critical. Decision points are also communication points as recovery and restoration decisions may or may not impact how our consortium partners operate and recover from adversity. Below is the process flow from event/ incident escalated to Disaster Recovery with recovery and post-mortem actions.



13 Appendix D: Continuous Improvement

Continuous improvement is essential to ensure the IT-Disaster Recovery Plan (IT-DRP) remains effective and up to date. This appendix outlines the processes and practices for ongoing enhancement of the plan.

13.1 Regular Reviews and Updates

- **Annual Review**: The IT-DRP should be reviewed and updated annually to incorporate lessons learned from exercises, actual incidents, and changes in the IT environment.
- **Post-Incident Analysis:** After any incident, a thorough analysis should be conducted to identify what worked well and what needs improvement. This analysis should result in actionable recommendations.
- **Feedback Mechanism:** Establish a feedback loop where team members can provide suggestions and insights based on their experiences during exercises and real incidents.

13.2 Maintenance, Testing, and Training

As referenced from the FFIECT IT Handbook, section VI, page 37 and section VII.A-VIII, pages 38-48.

In the rapidly evolving fintech landscape, ensuring resilience and continuity of operations is paramount. Maintaining and testing a robust Disaster Recovery Plan (DRP) is essential to safeguard critical assets and comply with regulatory requirements. This document outlines key best practices for the maintenance and testing of a DRP, providing a comprehensive approach to ensure preparedness and resilience in the face of potential disruptions.

Maintenance Best Practices

- **Regular Updates**: Treat the DRP as a living document. Regularly update it to reflect changes in technology, business processes, and organizational structure.
- **Documentation:** Ensure thorough documentation of all procedures, roles, and responsibilities. This includes maintaining an inventory of all critical assets and systems.
- **Stakeholder Involvement:** Engage representatives from different departments to ensure a holistic approach. This helps in identifying potential gaps and ensuring all critical areas are covered.
- **Compliance:** Regularly review the DRP to ensure it meets the latest NCUA and FFIEC guidelines and regulatory requirements.

Testing Best Practices

- **Regular Testing**: Conduct disaster recovery tests at least annually. This helps in identifying weaknesses and ensuring the plan's effectiveness.
- Varied Testing Methods:
    - Checklist Testing: Verify that all procedural details are comprehensive and account for necessary resources.
    - Walk-through Testing: Conduct step-by-step reviews with the disaster recovery team and stakeholders.
    - Simulation Testing: Role-play disaster scenarios to mimic real-world situations without disrupting business operations.
    - Full-Scale Simulation Testing: Execute the entire recovery process to assess the plan's effectiveness comprehensively.

- **Documentation of Tests**: Document all tests thoroughly, including outcomes and areas for improvement.
- **Metrics and Evaluation:** Define metrics to evaluate the effectiveness of the tests and make necessary adjustments based on the results.

Other Best Practices

- **Training:** Regularly train staff in their roles and responsibilities within the DRP to ensure readiness during an actual disaster.
- **Communication:** Maintain clear communication channels to ensure all stakeholders are informed and can coordinate effectively during a disaster.
- **Cross Training:** Ensure team members are cross-trained to handle multiple roles within the IT-Disaster Recovery teams

14 Glossary

The following are definitions relevant to this procedure.

Acronym/Term	Description
ATM	Automated Teller Machine
BC	Business Continuity
BCP	Business Continuity Plan
CIDS	Critical Incident Documentation Specialist
CIM	Critical Incident Manager
CIMP	Critical Incident Management Plan
CITM	Critical Incident Technical Manager
CU	Credit Union
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DBA	Database Administrator
FQDN	Fully Qualified Domain Name
ID	Identification
I/E	Insert/Extract
IP	Internet Protocol

Acronym/Term	Description
IVR	Interactive Voice Response
LCD	Liquid Crystal display
NATd	Network Address Translated
AnonCo	Anonymous Company, LLC
RAS	Remote Access Service
POS	Point of Sale
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SCSI	Small Computer Systems Interface
VSS	Volume Shadow (copy) Service