NOVEMBER 29, 2023

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

Table of Contents

NOVEMBER 29, 2023

Case Study

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

ConnectX (Mobile Services Provider Company)

1. Introduction

ConnectX is an innovative and forward-thinking mobile services provider, dedicated to transforming the way people connect and communicate in the digital era. Established in 2015, ConnectX has emerged as a dynamic force in the mobile industry, driven by a mission to redefine mobile communication through cutting-edge technology, exceptional customer experiences, and a commitment to positive social and environmental impact. With a vision to lead the way in connectivity, ConnectX is poised to shape the future of mobile services for individuals, families, and businesses across the globe.

2. Case Study

Physical Infrastructure:

ConnectX has invested significantly in its physical infrastructure to ensure a robust and reliable network that spans across urban, suburban, and rural areas. This infrastructure forms the backbone of its mobile communication services, enabling seamless connectivity for its customers.

ConnectX's headquarters in Pakistan serves as a strategic hub for its global operations. This modern office located in downtown Islamabad, spanning 6 floors, with each floor housing various departments and cutting-edge facilities:

Ground Floor (Floor 1): Customer Service Centre

- The grand entrance welcomes visitors and customers.
- Customer service representatives assist with inquiries, subscriptions, and support.

Floor 2: Customer Support

- The customer support centre manages technical inquiries, billing, and troubleshooting.
- Dedicated teams assist customers via phone and online channels.

Floor 3: Security Operations Centre

- A comprehensive security operations centre monitors access points, elevators, and critical areas.
- Security personnel respond to and manage security incidents.

Floors 4: Executive Offices

- The executive leadership team and administrative staff oversee company operations.
- Strategy and decision-making take place in these executive offices.

Floor 5: Network Operations

- Network engineers and technicians manage the company's global network infrastructure.
- This floor houses network equipment and monitoring stations.

Floor 6: Marketing and Sales

- The marketing and sales departments strategize and execute campaigns.
- Sales representatives work to acquire new customers and promote services.

The building is equipped with a comprehensive security system, including 500 CCTV cameras strategically placed to monitor access points, elevators, and critical areas.

IT Infrastructure and Services Details

ConnectX relies on a sophisticated IT infrastructure and a range of services to ensure the seamless operation of its mobile communication services. Here is an in-depth look at the key components:

1. Core Network Infrastructure:

Data Centres: ConnectX operates multiple state-of-the-art data centres, including one within its headquarters in Islamabad. These data centres are equipped with redundant power and cooling systems, fire suppression technology, and strict access controls to safeguard data and ensure high availability. They house critical networking equipment, servers, and databases that form the core of ConnectX's operations.

High-Speed Network Backbone: A high-speed, fibre-optic network backbone interconnects ConnectX's data centres, cell towers, and other critical infrastructure components. This network ensures fast and reliable data transmission between locations, supporting the delivery of voice, video, and data services.

2. Cloud Services:

Cloud Infrastructure: ConnectX utilizes cloud computing services to enhance scalability and flexibility. Virtualized resources in the cloud enable rapid deployment of new services and applications while efficiently managing server workloads.

Cloud-Based Data Storage: Critical data, including customer profiles and network configuration information, is securely stored in redundant cloud-based storage systems. This redundancy guarantees data integrity and high availability.

3. Customer-Facing Services:

Mobile Apps: ConnectX offers mobile apps for various platforms, providing customers with easy access to their accounts, billing information, and support services. These apps are designed for user-friendliness and compatibility with a wide range of devices.

Online Customer Portal: Customers can access an online portal to manage their accounts, view billing statements, and customize service plans. The portal also offers self-help resources and troubleshooting guides.

4. Network Monitoring and Management:

Network Operations Centre (NOC): ConnectX operates a 24/7 Network Operations Centre staffed by skilled engineers and technicians. The NOC monitors network performance, detects issues, and initiates rapid response and troubleshooting when necessary.

Remote Management Tools: Network administrators have access to remote management tools that allow them to configure and optimize network equipment, perform software updates, and troubleshoot issues remotely.

Employment details

ConnectX maintains a highly skilled and dedicated workforce to drive its success. Here are the employment details for ConnectX:

1. Network Engineers and Technicians:

ConnectX employs network engineers and technicians responsible for managing the company's network infrastructure, ensuring reliability and swift issue resolution.

2. Customer Service Representatives:

The customer service team provides round-the-clock support, assisting customers with inquiries, billing, and technical support.

3. Security Personnel:

A team of security experts oversees the safety of physical assets and data, monitoring access points and responding to security incidents.

4. IT Support Specialists:

IT support specialists ensure the smooth operation of IT infrastructure and resolve technical issues promptly.

5. Marketing and Sales Professionals:

The marketing and sales teams work diligently to promote ConnectX's services, acquire new customers, and tailor marketing campaigns.

Core Operations Details

1. **Technical Operations:**

Network Infrastructure: Design, deploy, and maintain a robust and high-performance mobile network infrastructure to ensure seamless connectivity for customers.

Hardware Maintenance: Regularly monitor and maintain network hardware, including cell towers, switches, and routers, to minimize downtime and disruptions.

Capacity Planning: Continuously assess network traffic and plan for capacity expansion t**o** meet growing demands.

Quality of Service (QoS): Implement QoS measures to ensure high-quality voice and data services for customers.

Troubleshooting: Rapidly respond to network issues and outages to minimize service disruptions.

2. **IT Operations:**

Customer Billing and Support Systems: Maintain billing systems and customer support platforms for accurate billing and efficient customer service.

OSS/BSS (Operations Support Systems/Business Support Systems): Manage OSS/BSS systems for network monitoring, inventory management, and customer relationship management.

IT Infrastructure: Ensure the reliability and security of the IT infrastructure, including servers, databases, and data centres.

Software Updates: Regularly update and patch software to protect against security vulnerabilities and improve service efficiency.

3. **Network Operations:**

Network Monitoring: Continuously monitor network performance, traffic, and security to identify and address issues proactively.

Capacity Management: Optimize network resources to ensure efficient usage and cost-effectiveness.

Vendor Management: Work with equipment vendors and service providers to maintain and upgrade network components.

4. **Financial Management:**

Budgeting and Financial Planning: Develop and manage budgets for various operational areas, including infrastructure investments and marketing expenses.

Revenue Assurance: Implement measures to prevent revenue leakage and ensure accurate billing.

Financial Reporting: Generate financial reports to track revenue, expenses, and profitability.

Business Working Methodology

1. Customer-Centric Focus

ConnectX prioritizes its customers at every stage of its operations. It employs advanced data analytics to segment customers and personalize services, ensuring a tailored approach to meet diverse needs.

2. Agile Network Management

ConnectX adopts an agile approach to network management, enabling rapid deployment of network upgrades and expansions in response to changing demand and technological advancements.

3. Innovation-Driven Strategy

ConnectX fosters a culture of innovation, regularly investing in research and development to stay at the forefront of technology. The company collaborates with technology partners to evaluate and deploy emerging technologies.

4. Localized Market Strategies

ConnectX tailors its market strategies to suit local preferences and market conditions. This includes adapting service plans, marketing campaigns, and customer support to meet specific geographic demands.

5. Continuous Employee Development

ConnectX places a strong emphasis on employee training and development. It offers ongoing learning opportunities to ensure that its workforce remains up to date with industry advancements.

6. Data-Driven Decision Making

ConnectX relies on data-driven decision-making processes. It collects and analyses data from various sources to make informed choices regarding network investments, service improvements, and customer engagement strategies.

7. Community Engagement

ConnectX actively engages with local communities through CSR (Corporate Social Responsibility) programs, supporting initiatives related to education, health, and social welfare

NOVEMBER 29, 2023

Asset Inventory

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

The Asset Inventory document serves as a comprehensive record of valuable resources owned by ConnectX. Managed by the Information Security Department and overseen by Senior Managers Muhammad Usman and Musaab Imran, this document captures crucial details about each asset, including its category, name, description, medium of storage, location, responsibility, date of purchase, purchase value, current value, condition, and external parties with access rights.

ConnectX's diverse assets encompass physical infrastructure, IT systems, software, personnel, and documentation. Examples range from the Headquarters Building in Islamabad, serving as the strategic hub for global operations, to the extensive network infrastructure, security systems, data centers, and various software applications crucial for daily operations.

To explore the complete and detailed Asset Inventory, please refer to the attached sheets (Information Security Management Plan Sheets) for a comprehensive understanding of ConnectX's valuable resources, their specifications, and the associated responsibilities and conditions. This inventory is vital for strategic planning, risk management, and ensuring the security and efficient functioning of ConnectX's operations.

NOVEMBER 29, 2023

Threat Analysis

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

The Threat Analysis for ConnectX identifies a spectrum of potential risks across its diverse assets. From physical break-ins to insider threats and the looming danger of natural disasters, the analysis covers various dimensions of vulnerability. For instance, the threat of unauthorized access to the headquarters building, deliberate destruction of office furniture, and the risk of fire hazards underscores the need for robust security measures. Additionally, concerns extend to malfunctions in critical systems, potential data breaches, and the overarching menace of identity theft. This comprehensive assessment acts as a strategic guide for implementing targeted security protocols, ensuring ConnectX's resilience against a wide array of potential threats to its assets. For detailed insights into specific threats associated with each asset category, please refer to the complete Threat Analysis document. To explore the complete and detailed Asset Inventory, please refer to the attached sheets (Information Security Management Plan Sheets)

NOVEMBER 29, 2023

Risk Assessment

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

The risk assessment sheets provide a comprehensive overview of the potential risks associated with various assets within ConnectX. The assets are evaluated based on their confidentiality, integrity, and availability (CIA) scores, considering factors such as value, classification, and specific remarks. Additionally, each asset is assessed for exposure by identifying existing controls, potential threats, vulnerability descriptions, and the probability of exposure. The impact/severity rating is also calculated to quantify the potential consequences of a security incident.

For instance, the Mobile App, a critical asset with high usage and customer interaction, is evaluated for potential risks such as unavailability of services and server overload. The risk exposure is then determined, and control measures, such as load balancing techniques, are recommended.

These risk assessment sheets serve as valuable tools for identifying, analysing, and addressing potential security risks, allowing ConnectX to implement effective security measures and safeguards. For detailed information and specific recommendations, please refer to the attached risk assessment sheets in (Information Security Management Plan Sheets).

NOVEMBER 29, 2023

Enterprise Information Security Policy (EISP)

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

Enterprise Information Security Polic (EISP):

1. Purpose

ConnectX, as an innovative mobile services provider in Pakistan, recognizes the paramount importance of safeguarding information in the digital age. The Purpose of this Enterprise Information Security Policy is to articulate ConnectX's unwavering commitment to preserving the confidentiality, integrity, and availability of information assets. Established against the backdrop of Pakistan's dynamic regulatory landscape, this Policy serves as a guiding framework, ensuring compliance with local laws, fostering customer trust, and fortifying the foundations of ConnectX's digital ecosystem.

2. Authority

ConnectX derives its legal authority for information technology activities from a comprehensive understanding of Pakistani laws and regulations governing the telecommunications sector. The policy aligns with the mandates of the Pakistan Telecommunication Authority (PTA) and other relevant regulatory bodies. This legal foundation empowers ConnectX to conduct its operations in adherence to the country's norms, ensuring the lawful and ethical use of information.

3. Scope

The scope of this policy is specifically limited to the information technology (IT) assets within ConnectX's operations in Pakistan. It recognizes and adheres to the specific regulatory requirements imposed by the Pakistan Telecommunication Authority (PTA). The policy focuses solely on aspects related to information security, encompassing information systems, electronic devices, and network resources utilized in the provision of mobile communication services. By design, this policy is tailored to the unique features of Pakistan's information security landscape, ensuring a clear and compliant framework for IT operations.

4. Responsibility

The Enterprise Security Office (Information Security Department) at ConnectX Islamabad headquarters, Pakistan serves as the fulcrum for policy development and maintenance. Tasked with comprehensively understanding the evolving regulatory landscape and the specific needs of ConnectX's operations in Pakistan, the office ensures that the policy is a living document, responsive to changes in technology, law, and business dynamics.

5. Compliance

The Enterprise Security Office (Information Security Department) at ConnectX holds the responsibility of overseeing compliance with this policy. Collaboration with various departments is integral to ensure a cohesive approach to compliance, and periodic audits are conducted to verify adherence. The initiative-taking engagement of the office with regulatory authorities ensures a dynamic understanding of compliance requirements.

ConnectX also recognizes the mandatory nature of compliance with this policy. Violations are treated with utmost seriousness, as outlined in employment and collective bargaining agreements. Ensuring alignment with Pakistani employment laws, the policy establishes a clear framework for disciplinary actions, including potential termination in cases of severe violations.

6. Information Security Objectives

6.1. Enable Organizational Strategy:

ConnectX aims to align its information security measures with its organizational strategy, particularly focusing on the protection of customer data and material non-public information. This objective underscores ConnectX's commitment to develop trust among its customer base and leveraging information security as a strategic enabler.

6.2. Regulatory Compliance:

Adherence to applicable Pakistani laws, regulations, and contractual obligations is paramount. ConnectX commits to robust processes and controls to ensure ongoing compliance, recognizing the importance of maintaining trust with regulatory bodies, stakeholders, and customers.

6.3. Governance Structure:

Establishing a governance structure specific to the Pakistani context is a critical objective. ConnectX aims to create an effective and efficient mechanism for managing information security risks, considering the unique regulatory nuances of the Pakistani technology landscape.

6.4. Risk Management:

Managing identified security risks to an acceptable level is foundational to ConnectX's information security strategy. Through robust risk assessment, mitigation planning, and ongoing monitoring, ConnectX seeks to strike a balance between innovation and risk avoidance, aligning with the risk tolerance parameters set by Pakistani regulatory authorities.

6.5. Culture of Accountability:

ConnectX promotes to establish a culture of accountability and awareness among all personnel. This objective recognizes the importance of fostering a security-conscious culture, ensuring that every employee plays an active role in meeting information security requirements.

6.6. Responsibility and Accountability:

ConnectX commits to establishing clear lines of responsibility and accountability for information security policies and governance. This objective aligns with the broader

organizational structure, ensuring that information security is a shared responsibility throughout ConnectX Pakistan.

7. Communications

ConnectX acknowledges the importance of transparency in its operations and the need for public awareness. To strike a balance between transparency and security, the company provides a summarized version or high-level overview of its Information Security policies and standards, making them selectively available to the public. Access to this information is facilitated through controlled channels, ensuring that essential security measures are communicated without exposing intricate details. This approach aligns with industry best practices and regulatory considerations in Pakistan, where there is a growing emphasis on corporate transparency and stakeholder engagement.

8. Reporting Requirements

8.1. Policy Violations:

ConnectX has developed a robust reporting mechanism for policy violations. The reporting process follows applicable employment and collective bargaining agreements, ensuring a fair and consistent approach to addressing violations. This approach is in line with Pakistan's Labor laws, emphasizing procedural fairness.

8.2. Reporting of Policy Violations:

The reporting process for policy violations is structured to encourage swift reporting. This includes reporting to immediate supervisors and the Information Security Team. The process is enhanced with the broader regulatory framework, ensuring that any security incidents are promptly reported to the relevant authorities.

8.3. Exceptions from Policy:

Recognizing that there might be scenarios where strict adherence to policy is not feasible, ConnectX has established a framework for exceptions. This includes a clear process for submitting and approving policy exception requests, with the final decision resting with the Commonwealth CISO, Deputy CISO, or their delegate. This aligns with the flexibility often required to navigate the evolving regulatory landscape in Pakistan.

9. Policy Statement

9.1. Acceptable Use Policy

9.1.1. General Use and Ownership

9.1.1.1. ConnectX Proprietary Information

ConnectX's proprietary information, including critical data such as customer profiles and network configurations, is the lifeblood of its operations. Given its commitment to customer privacy and satisfaction, ConnectX enforces protection

measures in line with the Data Protection Standard. This ensures that customer data remains secure and is managed responsibly.

9.1.1.2. Prompt reporting of theft, loss, or unauthorized disclosure

ConnectX operates a Security Operations Centre that actively responds to and manages security incidents. In the event of a breach, employees are obligated to promptly report any theft, loss, or unauthorized disclosure of proprietary information. This initiative-taking approach aligns with ConnectX's dedication to maintaining the integrity and security of its operations.

9.1.1.3. Access, use, or share proprietary information.

With a diverse range of roles such as customer service, security, and network management, ConnectX emphasizes the principle of least privilege. Access to proprietary information is restricted to authorized personnel, ensuring that employees only access information necessary for fulfilling their assigned job duties. This ensures a balance between operational needs and data security.

9.1.1.4. Exercise of good judgment for personal use

ConnectX acknowledges the varied responsibilities of its employees, including customer service, security, and network management. The policy encourages employees to exercise good judgment in the personal use of company resources, aligning with departmental policies. This commitment reflects ConnectX's responsibility to ensure the responsible and ethical use of its resources.

9.1.1.5. Monitoring by authorized individuals

ConnectX's commitment to network security is evident through its Network Operations Centre, operating 24/7. The policy recognizes that authorized individuals may monitor equipment, systems, and network traffic at any time for security and maintenance purposes. This initiative-taking approach ensures the company's ability to swiftly respond to emerging threats.

9.1.1.6. Right to audit networks and systems

ConnectX's significant investment in IT infrastructure, data centers, and cloud services underscores the importance of robust network and system management. The policy grants ConnectX the right to audit networks and systems periodically, ensuring ongoing compliance with information security policies. This reflects a commitment to transparency and accountability in security practices.

9.1.2. Security and Proprietary Information

9.1.2.1. Compliance with Minimum Access Policy

ConnectX has a comprehensive security system with resolute security personnel. To maintain a consistent security posture, the policy mandates that all mobile and computing devices connecting to the internal network comply with the Minimum

Access Policy. This approach ensures a unified and secure access control framework.

9.1.2.2. Password Policy

Security measures such as monitoring, data center security, and access controls are emphasized in the case study. Passwords used in ConnectX must comply with the Password Policy, ensuring secure access to systems and aligning with best practices in password management. This ensures that user credentials, a critical aspect of information security, meet industry standards.

9.1.2.3. Password-protected lock screen

ConnectX's focus on security is evident through a Security Operations Centre and network monitoring. The policy mandates that all computing devices used in ConnectX must have a password-protected lock screen with automatic activation within a specified timeframe. This security measure ensures protection against unauthorized access and aligns with industry best practices.

9.1.2.4. Disclaimer in postings from ConnectX email address

ConnectX engages in marketing and sales through dedicated departments. The policy requires that postings from a ConnectX email address to newsgroups or online platforms contain a disclaimer. This aligns with ConnectX's commitment to transparent and responsible communication, ensuring that online communications are clearly distinguished as personal opinions.

9.1.2.5. Caution in opening email attachments

ConnectX utilizes cloud-based storage for critical data. Employees are mandated to use caution when opening email attachments to avoid malware. This aligns with best practices for data security employed by ConnectX and reinforces the importance of maintaining the integrity and security of the company's information assets.

9.1.3. Unacceptable Use

9.1.3.1. System and Network Activities

ConnectX's focus on innovation and technology partnerships aligns with this policy. Prohibited activities include unauthorized access, security breaches, and malicious program introduction. This ensures that ConnectX operates within legal and ethical boundaries, fostering a secure and compliant working environment.

9.1.3.2. Email and Communication Activities

ConnectX offers customer-facing services through mobile apps and an online portal. Prohibited activities include unsolicited email messages and harassment, ensuring responsible use of company resources and aligning with customer-centric

values. This reinforces ConnectX's commitment to providing a secure and respectful communication environment.

9.1.3.3. Blogging and social media

ConnectX emphasizes community engagement through CSR programs. Blogging or posting to social media platforms is allowed with restrictions to protect company interests. This reflects ConnectX's commitment to community engagement and responsible social media use. The policy ensures that employee interactions online align with the company's values and ethical standards.

9.2. Database Credentials Policy

9.2.1. General:

- ConnectX ensures the security of its internal databases by implementing access through authenticated credentials.
- Database credentials are not stored in the main executing body of program source code in clear text or easily reversible encryption, aligning with policy requirements.
- Algorithms used for database authentication at ConnectX meet or exceed the standards defined in NIST publication FIPS 140-2, with a strong recommendation for the use of RSA and Elliptic Curve Cryptography (ECC) algorithms for asymmetric encryption.

9.2.2. Specific Requirements:

- Database usernames and passwords at ConnectX are stored in a file separate from the executing body of the program's code, ensuring confidentiality.
- The file containing database credentials is not world-readable or writeable, enhancing security.
- Alternatively, ConnectX may store database credentials on the database server with a hash function number identifying the credentials stored in the executing body of the program's code.
- Authentication servers, such as LDAP servers, are utilized for database authentication, eliminating the programmatic use of database credentials.
- Passwords or passphrases used for database access at ConnectX adhere to the Password Policy.

9.2.3. Retrieval of Database Usernames and Passwords:

If stored in a separate file, database usernames and passwords at ConnectX are read immediately prior to use, and memory containing this information is released or cleared post-authentication.

9.2.4. Access to Database Usernames and Passwords

- Every program or collection of programs at ConnectX implementing a single business function has unique database credentials, complying with the policy's restriction on sharing credentials between programs.
- Database passwords used by programs at ConnectX are treated as system-level passwords, aligning with the Password Policy.

- ConnectX has a process in place to control and change database passwords in accordance with the Password Policy, ensuring restricted knowledge of passwords to a need-to-know basis within developer groups.
- Users and/or software at ConnectX accessing sensitive data are subjected to proper access control, preventing the performance of privileged operations outside their scope.

9.3. Email Policy

9.3.1. Consistency with Policies and Ethical Conduct:

ConnectX emphasizes that all email usage must align with the company's policies, ethical conduct guidelines, safety protocols, and compliance with relevant laws and business practices. This ensures that employee behaviour through email communication reflects the company's values and legal obligations.

9.3.2. Primary Use for Business Purposes:

ConnectX email accounts serve as a primary means for official business-related communication. While limited personal use is permitted, employees are reminded that engaging in non-ConnectX related commercial activities through the company's email system is prohibited.

9.3.3. Data Protection Standard:

The security of ConnectX's data is important. All information within email messages or attachments must adhere to the Data Protection Standard, guaranteeing the confidentiality and integrity of sensitive data. This policy underscores ConnectX's commitment to safeguarding its proprietary information.

9.3.4. Retention of Business Records:

ConnectX establishes guidelines for the retention of emails. Only those emails qualifying as business records, with a legitimate and ongoing business reason for preservation, should be retained. The company follows a Record Retention Schedule to ensure compliance with regulatory requirements and should be compliance with email retention policy.

9.3.5. Prohibition of Disruptive or Offensive Messages:

ConnectX sets a clear expectation that the email system is not a platform for creating or distributing disruptive or offensive messages. This includes content that may be offensive based on race, gender, or other protected characteristics. Employees encountering such content are urged to report it promptly.

9.3.6. Prohibition of Automatic Forwarding:

To prevent unauthorized disclosure, users are prohibited from automatically forwarding ConnectX email to external third-party systems. Any manual forwarding

should exclude ConnectX confidential information, ensuring the security of sensitive data.

9.3.7. Reasonable Personal Use:

Acknowledging that employees may use company resources for personal emails within reason, ConnectX encourages responsible and limited personal use. Clear guidelines prohibit the sending of chain letters or joke emails through the ConnectX email accounts.

9.3.8. No Expectation of Privacy:

ConnectX communicates that employees should have no expectation of privacy concerning their use of the company's email system. This aligns with the company's commitment to monitoring and ensuring the security of its communication channels.

9.3.9. Monitoring and Notice:

ConnectX reserves the right to monitor email messages without prior notice. This proactive approach is taken to maintain the security of the company's email system and emphasizes that employees should not assume privacy regarding their email correspondence.

9.4. Email Retention Policy

9.4.1. Administrative Correspondence:

- ConnectX designates Administrative Correspondence for internal communications, including policy clarification, holidays, timecard information, dress code, workplace behaviour, and legal issues.
- All emails labelled "Management Only" fall under this category.
- Retention is administered through a dedicated mailbox, such as admin@connectx.

9.4.2. Fiscal Correspondence:

- Fiscal Correspondence at ConnectX encompasses information related to revenue and expenses.
- A designated mailbox, like fiscal@connectx, is employed for retention and administration by the IT Department.

9.4.3. General Correspondence:

- ConnectX's General Correspondence includes information relating to customer interaction and operational decisions.
- Individual employees are responsible for the retention of General Correspondence.

9.4.4. Ephemeral Correspondence:

- Ephemeral Correspondence constitutes a broad category, covering personal emails, requests, product development-related emails, updates, and status reports.
- No specific retention measures are outlined, placing the responsibility on individual employees.

9.4.5. Encrypted Communications:

- ConnectX emphasizes storing encrypted communications in a manner consistent with its Information Sensitivity Policy.
- The recommendation is to store information in a decrypted format.

9.4.6. Recovering Deleted Email via Backup Media:

- ConnectX follows a practice of maintaining backup tapes for email recovery.
- Email recovery efforts are not made to remove emails from offsite backup tapes.

9.4.7. General Standards:

- Approved Electronic Mail, Encrypted Email and Files, Approved Instant Messenger, and Individual Access Controls are integral parts of ConnectX's general standards.
- Specific tools and controls should be highlighted for each category.

9.5. Web Application Security Policy

9.5.1. Web Application Security Assessments:

- **New or Major Application Release:** ConnectX web applications undergoing significant changes will undergo a full security assessment before approval for deployment.
- **Third Party or Acquired Web Application:** Third-party or acquired web applications will undergo a complete security assessment to ensure compliance with ConnectX policy requirements.
- **Point Release:** Depending on risk factors associated with changes in functionality or architecture, point releases will undergo an appropriate level of security assessment.
- **Patch Releases:** Patch releases will undergo security assessments based on the risk associated with changes to application functionality or architecture.
- **Emergency Releases:** Emergency releases, exempt from pre-assessment, will be designated by the Chief Information Officer or a delegated manager. They will carry assumed risk until a proper assessment can be conducted.
- **Annual Review:** All web applications will undergo a comprehensive annual review to identify and mitigate potential risks related to functionality and architecture.

9.5.2. Security Issue Mitigation:

- **High-Risk Issues:** High-risk issues demand immediate resolution or implementation of mitigation strategies to limit exposure. Applications with high-risk issues may be taken offline or denied release until addressed.

- **Medium-Risk Issues:** Medium-risk issues will be reviewed to determine necessary mitigation and scheduled accordingly. Multiple medium-risk issues may impact release approval, and fixes should be implemented in a patch or point release.
- **Low-Risk Issues:** Low-risk issues will be reviewed for correction, with scheduling based on their severity.

9.5.3. Security Assessment Levels:

- **Full Assessment:** Full assessments involve comprehensive testing for all known web application vulnerabilities, combining automated and manual tools based on the OWASP Testing Guide.
- **Quick Assessment:** Quick assessments, typically automated, focus on identifying the OWASP Top Ten web application security risks at a minimum.
- **Targeted Assessment:** Targeted assessments verify vulnerability remediation changes or validate new application functionality.

9.5.4. Approved Assessment Tools:

ConnectX utilizes approved web application security assessment tools, including:

- **Burp Suite Professional:** A comprehensive platform for web application security testing.
- **Nessus Professional:** An advanced vulnerability scanner to identify and remediate web application vulnerabilities.
- **OWASP ZAP:** An open-source security testing tool to find vulnerabilities in web applications.

Additional tools or techniques may be employed based on assessment findings and risk evaluation by the Security Engineering team.

9.6. Server Security Policy

9.6.1. General Requirements:

- **Server Ownership and Configuration:**
  - All internal servers at ConnectX must be owned by operational groups responsible for system administration.
  - Approved server configuration guides must be established, maintained, and reviewed by the InfoSec team based on business needs.
  - Servers must be registered in the corporate enterprise management system with essential information, including contacts, hardware, OS/version, functions, and applications.
  - Information in the management system must be kept up to date.
  - Configuration changes for production servers must follow change management procedures.
- **Monitoring and Auditing:**

Authorized personnel may monitor and audit equipment, systems, processes, and network traffic for security, compliance, and maintenance purposes following the Audit Policy.

9.6.2. Configuration Requirements:

- **Operating System Configuration:**

  OS configuration must align with InfoSec team guidelines.

- **Services and Applications:**

  Disable unused services and applications for security.

- **Access Control and Logging:**
  - Log and protect access to services using methods like a web application firewall.
  - Install the latest security patches promptly, with exceptions allowed only when immediate application interferes with business requirements.
  - Avoid trust relationships between systems as they pose security risks.
  - Apply standard security principles, using the least required access.
  - Privileged access should be performed over secure channels (e.g., encrypted network connections using SSH or IPsec).
  - Physically locate servers in an access-controlled, secured environment, prohibiting operation from uncontrolled or unsecured cubicle areas.

9.6.3. Monitoring:

- **Security-Related Event Logging:**
  - Log all security-related events on critical or sensitive systems.
  - Retain online logs for a minimum of 1 week, daily incremental tape backups for at least 1-month, weekly full tape backups for at least 1 month, and monthly full backups for a minimum of 2 years.
- **Incident Reporting:**
  - Report security-related events to InfoSec for review and incident reporting to IT management.
  - Security-related events include port-scan attacks, evidence of unauthorized access to privileged accounts, and anomalous activities.

9.7. Data Breach Response Policy

9.7.1. Incident Identification and Response Team Formation:

- Upon identifying a theft, breach, or exposure of ConnectX Protected or Sensitive data, all access to the affected resource will be promptly removed.
- The Executive Director will lead an incident response team, including members from IT Infrastructure, IT Applications, Finance, Legal, Communications, Member Services, Human Resources, and the affected unit or department.

- Additional departments and individuals may be included based on the data type involved.

9.7.2. Notification and Analysis:

- The Executive Director will be notified of the incident, and IT, along with a forensic team, will analyse the breach to determine the root cause.
- Forensic investigators, provided by ConnectX cyber insurance, will determine how the breach occurred, the types of data involved, and the impact on individuals and organizations.

9.8. Password Construction Policy

9.8.1. Password Strength Recommendations:

- All ConnectX employees must use strong passwords to access company systems.
- Strong passwords are characterized by a minimum of 16 characters.

9.8.2. Use of Passphrases:

- Employees are encouraged to use passphrases, which are combinations of multiple words, as they are both easy to remember and type.
- Passphrases should meet the minimum strength requirements and can include spaces between words.
- Examples include 'It’s time for vacation' or 'block-curious-sunny-leaves'.

9.8.3. Periodic Password Cracking or Guessing:

- The Information Security (InfoSec) Team or its delegates may conduct periodic or random password cracking or guessing scans.
- In the event of a guessed or cracked password during these scans, the user will be required to change their password promptly.

9.9. Password Protection Policy

9.9.1. Password Creation and Use:

- **Password Construction Guidelines:** All user-level and system-level passwords must adhere to the Password Construction Guidelines, ensuring robust and secure password structures.
- **Unique Passwords**: Users are required to maintain separate and unique passwords for each work-related account, preventing the use of work-related passwords for personal accounts.
- **Password Management:** Staff members are permitted to use authorized password managers to securely store and manage their work-related passwords, promoting secure password practices.
- **Privileged Accounts:** User accounts with system-level privileges must have unique passwords. Additionally, it is strongly recommended to implement multi-factor authentication for added security.

9.9.2. Password Change:

- **Password Change Policy:** Passwords should only be changed when there is a reasonable belief that a password has been compromised or does not meet the Password Creation Requirements.
- **Expiration Recommendations:** Regular password expiration is not recommended, promoting a more user-friendly approach while maintaining security.

9.9.3. Password Protection:

- **Confidentiality:** Passwords must be kept confidential, and sharing with anyone, including supervisors and coworkers, is prohibited. All passwords are treated as sensitive and confidential ConnectX information.
- **Communication Channels:** Passwords must not be inserted into email messages or disclosed over the phone. They may only be stored in organization-approved password managers.
- **"Remember Password" Feature:** The use of the "Remember Password" feature in applications, such as web browsers, is prohibited to enhance security.
- **Incident Reporting:** Any individual suspecting a compromised password must promptly report the incident and change all relevant passwords to mitigate potential risks.

9.9.4. Application Development:

- **Authentication Support:** Applications must support the authentication of individual users, emphasizing the importance of user-specific access.
- **Password Storage:** Passwords must not be stored in clear text or any easily reversible form within applications, ensuring data security.
- **Network Transmission:** The transmission of passwords in clear text over the network by applications is prohibited to prevent unauthorized access.

9.9.5. Multi-Factor Authentication:

- Multi-factor authentication is highly encouraged and should be implemented whenever possible, not only for work-related accounts but also for personal accounts, enhancing overall account security.

9.10.Employee Internet Use Monitoring and Filtering Policy

9.10.1. Web Site Monitoring

- The Information Technology (IT) Department at ConnectX is responsible for the continuous monitoring of Internet use across all computers and devices connected to the corporate network.
- The monitoring system employed must meticulously record crucial details for all network traffic, including the source IP Address, date, time, protocol, and destination site or server. Additionally, the system should endeavour to capture the User ID of the individual initiating the respective traffic.
- To comply with legal and security requirements, Internet Use records must be diligently preserved for a duration of 180 days.

9.10.2. Internet Use Filtering System

- The Information Technology Department shall deploy a comprehensive filtering system designed to block access to Internet websites and protocols that are deemed inappropriate for ConnectX's corporate environment.

The following protocols and categories of websites are subject to blocking:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Chat and Instant Messaging
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- Personals and Dating
- Social Network Services
- SPAM, Phishing and Fraud
- Spyware
- Tasteless and Offensive Content
- Violence, Intolerance and Hate
- Web-Based Email

9.10.4. Internet Use Filtering Rule Changes

- The Information Technology Department will conduct regular reviews and recommend changes to web and protocol filtering rules to adapt to evolving security needs.
- Human Resources will thoroughly evaluate these recommendations and make decisions regarding necessary changes, with all modifications being meticulously recorded in the Internet Use Monitoring and Filtering Policy.

9.10.5. Internet Use Filtering Exceptions

- In cases where a site is mis-categorized, employees have the right to request unblocking by submitting a ticket to the Information Technology help desk.
- IT personnel will promptly review such requests and unblock the site if it is determined to be mis-categorized.
- Employees may access blocked sites with explicit permission for legitimate business purposes. Requests for such access must be submitted to their Human Resources representative.
- HR will compile and present all approved exception requests to Information Technology in writing or by email. Information Technology will then proceed to unblock the site or category exclusively for the requesting associate.

- A comprehensive record of approved exceptions will be maintained by Information Technology, and reports on these exceptions will be provided upon request.

10. Policy Framework Coverage

ConnectX ensures a comprehensive alignment of its policies with the EISP framework. This alignment extends to various critical topics, including organization, acceptable use, access management, asset management, and more. The objective is to create a cohesive policy architecture that mirrors the regulatory framework of Pakistan, ensuring a robust and integrated approach to information security.

11. Document Change Control

11.1. Document Versions:

ConnectX maintains a version control system, documenting changes, and updates to the Enterprise Information Security Policy. This detailed versioning serves as an audit trail, reflecting the company's commitment to transparency and accountability. Each version is accompanied by a comprehensive description of changes, providing clarity on the evolution of the policy. A bird eye view of versions is listed below:

Version No.	Revised by	Effective date	Description of changes
0.80	Ali Khan	10/01/2017	Initial Draft
0.90	Fatima Ahmed	12/18/2017	Minor corrections, wording
1.0	Ahmed Hassan	5/31/2018	Finalized content and pre-publication review
1.1	Usman Ali	08/29/2022	Results of Internal Audit and minor revisions
1.2	Musaab, Usman	30/11/2023	Annual Review with minor additions.

11.2. Annual Review:

ConnectX Pakistan recognizes the dynamic nature of the regulatory environment and commits to an annual review of the Enterprise Information Security Policy. This review is not only a proactive measure to ensure ongoing compliance but also an opportunity to incorporate feedback, assess emerging risks, and align the policy with any changes in the Pakistani regulatory landscape.

Additionally, document updates are initiated in response to internal and external audits, ensuring continuous improvement and adaptability to evolving security requirements.

12. Definitions:

Term	Definition
Proprietary Information	Critical data owned exclusively by ConnectX, including customer profiles and network configurations.
Password Policy	ConnectX's guidelines for creating and managing secure passwords, ensuring protected access to systems.
Security Operations Centre (SOC)	Dedicated facility monitoring, responding to, and managing security incidents for ConnectX.
Cloud-Based Storage	Service for securely storing critical data, ensuring integrity and availability in redundant cloud systems.
Network Monitoring	Continuous surveillance of network performance by ConnectX's Network Operations Centre (NOC).
CSR Programs	Initiatives by ConnectX engaging with and supporting local communities, focusing on positive contributions.
Community Engagement	ConnectX's involvement in activities fostering positive relationships with local communities.
Database Credentials	Authentication information, including usernames and passwords, required to access and interact with a database.
Asymmetric Encryption	A cryptographic method using pairs of public and private keys for secure communication between two parties.
Hash Function Number	A numerical representation derived from a hash function, often used to uniquely identify sensitive information.
LDAP Server	Lightweight Directory Access Protocol server, utilized for centralized management of user authentication.
Password Policy	A set of rules and guidelines defining the criteria for creating, changing, and handling passwords securely.
System-Level Password	A password used for critical system functions, meeting higher security standards, as defined in the Password Policy.
encryption or Encrypted Data	The most effective method for data security, requiring a secret key or password for decryption.
Plain Text	Data in an unencrypted form.
Hacker	A computer enthusiast or expert in programming languages and computer systems.
PII (Personally Identifiable Information)	Data that could potentially identify a specific individual.
Protected Data	Includes PII and PHI, emphasizing information requiring special protection due to its sensitivity.
Information Resource	The data and information assets of ConnectX.
Safeguards	Countermeasures or controls implemented to avoid, detect, counteract, or minimize security risks.
Sensitive Data	Refers to encrypted or plain text data containing PII or PHI data, emphasizing the need for heightened security measures.
Privileged Accounts	User accounts with system-level privileges, requiring unique passwords and recommending multi-factor authentication.

NOVEMBER 29, 2023

Contingency Plan

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

Incident Response Plan

1. Planning Phase

1.1. Introduction

General information:

This manual has been developed for "ConnectX" herein referred to as "ConnectX," and is considered the confidential property of the entity. Due to the sensitive nature of the information contained herein, access to this manual is restricted to individuals designated as members of incident management teams or those directly involved in incident response and recovery processes.

Unless otherwise instructed, each plan recipient is responsible for maintaining two copies of the plan, one at their office and one at their home. For additional copies, contact 03227118856.

The following teams will be referenced throughout this plan:

1. Threat Assessment Centre
2. Regional Incident Management Team
3. Damage Assessment Team
4. Local Incident Management Team

The incident management planning effort for ConnectX recognizes the importance of people, processes, and technology to the corporation. It is the responsibility of every ConnectX manager and employee to safeguard and maintain the confidentiality of all corporate assets.

1.2. Incident Response Plan Overview

Overview and Objectives:

This incident management plan establishes the recommended organization, actions, and procedures needed to:

1. Recognize and respond to an incident.
2. Quickly and effectively assess the situation.
3. Notify appropriate individuals and organizations.
4. Organize the company’s response activities, including activating a command centre.
5. Escalate response efforts based on incident severity.
6. Support business recovery efforts after the incident.

This plan aims to minimize operational and financial impacts of disasters and will be activated when a local Incident Manager determines that a disaster has occurred. Specific details on incident response and subsequent business recovery actions are outlined in local recovery team plans.

1.3. Scope

This incident management plan covers initial actions and procedures to respond to events impacting critical business activities at ConnectX headquarters. It is designed to minimize operational and financial impacts of disasters.

The plan responds to any unplanned business interruption, such as a loss of utility service, avian influenza outbreak, or catastrophic events like a major fire or flood.

1.4. Exclusions

This plan excludes facilities not located at ConnectX headquarters (Islamabad).

1.5. Planning Scenarios

This plan addresses incidents that could render ConnectX headquarters out of service or inaccessible, including:

1. No access to buildings or floors
2. Loss of data communications and network infrastructure
3. Loss of technology
4. Loss of professional staff

1.5.1. Limited or No Access to the Building:

Any incident rendering ConnectX headquarters either totally or partially inaccessible, impacting workspaces and requiring incident management and recovery actions.

1.5.2. Loss of Data Communications:

Any incident disabling or destroying WAN router infrastructure, affecting business operations, and requiring recovery strategies.

1.5.3. Loss of Technology:

Any incident disabling or destroying the entire computer room facility, impacting business operations, and requiring recovery strategies.

1.5.4. Loss of People:

Any incident disabling or rendering professional staff unable to perform normal functions, impacting business operations and potentially requiring temporary staff.

1.6. Recovery Objectives

This incident management plan aims to:

- Provide an organized and consolidated approach to managing initial response and recovery activities.
- Respond promptly to unplanned incidents, reducing short-term business interruptions.
- Notify relevant stakeholders of the incident.
- Recover essential business operations in a timely manner.

1.7. Assumptions

This plan is based on the assumptions that:

- A complete interruption of ConnectX headquarters has occurred.

- Loss of professional staff has occurred due to a disaster, and only a limited number of healthy employees are available.
- Recovery from anything less than a complete interruption will use appropriate portions of this plan.
- Sufficient staff with adequate knowledge will be available for recovery.

2. Contact Information

Contact Information:

Name	Title	Role	Contact Information	Escalation *(1-3)
Ali Khan	Information Security Manager	IR Commander, CSIRT Manager	ali.khan@connectx.com / 123-456-7890	1
Ayesha Malik	Infrastructure Manager	IR Manager	ayesha.malik@connectx.com / 987-654-3210	1
Fahad Ahmed	Chief Information Officer (CIO)	CIO	fahad.ahmed@connectx.com / 555-123-4567	2
Hira Mahmood	Communications Manager	IHT Member	hira.mahmood@connectx.com / 222-333-4444	3
Imran Abbas	Legal	IHT Member	imran.abbas@connectx.com / 999-888-7777	3
Safiya Khan	Risk Manager	IHT Member	safiya.khan@connectx.com / 444-555-6666	3
Ahmed Raza	HR Representative	IHT Member	ahmed.raza@connectx.com / 777-888-9999	3
Farida Ali	Physical Security Representative	IHT Member	farida.ali@connectx.com / 111-222-3333	3
Bilal Akram	3rd Party Support		bilal.akram@connectx.com / 123-987-4567	3
Nida Hassan	Cyber Insurance Provider		nida.hassan@connectx.com / 456-789-0123	3

*Escalation level determines order in which notification should occur:

1. Notify first, required on all incidents.
2. Required on all moderate or high severity incidents.
3. Involve as needed.

*Incase email worn work we will shift to slack and WhatsApp.

3. Assembly Area

- Primary Assembly Area:
  - Name: ConnectX Headquarters
  - Address: 123 Main Street
  - City/State/Zip: Islamabad, ISB, 44000
  - Phone/Fax: +92 345 678 901 / +92 345 678 902
  - Email: headquarters@connectx.com

- Secondary Assembly Area:
  - Name: ConnectX Secondary Office
  - Address: 456 Central Avenue
  - City/State/Zip: Islamabad, ISB, 44001
  - Phone/Fax: +92 345 678 903 / +92 345 678 904
  - Email: secondary.office@connectx.com
- Tertiary Assembly Area:
  - Name: ConnectX Tertiary Office
  - Address: 789 Downtown Boulevard
  - City/State/Zip: Islamabad, ISB, 44002
  - Phone/Fax: +92 345 678 905 / +92 345 678 906
  - Email: tertiary.office@connectx.com

4. Roles & Responsibilities

4.1.Cyber Security Incident Handling Team (IHT)

Team Composition for ConnectX:

Legal experts, risk managers, and other department managers relevant to incident response.

Roles and Responsibilities:

- Advise on incident response activities related to their expertise.
- Maintain a general understanding of ConnectX's incident response plan and policies.
- Ensure incident response aligns with legal, contractual, and regulatory requirements.
- Participate in tests of the incident response plan.
- Manage internal and external communications during cybersecurity incidents.

4.2.Chief Information Officer (CIO/CTO)

Roles and Responsibilities:

- Seek approval from Executive Management for the administration of the Incident Response Program.
- Coordinate response activities with auxiliary departments and external resources.
- Provide updates on response activities to the Incident Handling Team (IHT) and other stakeholders.
- Ensure service level agreements with service providers define expectations for incident response.
- Review and seek approval for the Cyber Security Incident Response Plan.
- Collaborate with the IR Commander to evaluate the effectiveness of the Plan and CSIRT periodically.
- Approve the closure of moderate or critical-severity incidents.
- Oversee Cyber Insurance maintenance and inform appropriate stakeholders.
- Ensure lessons learned are applied for Severity 1 incidents.

4.3.Cyber Security Incident Response Team (CSIRT)

List of Team Members

No.	CSIRT Member	Role
1	Ali Khan	IR Commander
2	Sara Ahmed	Incident Response Team Member
3	Fahad Malik	Incident Response Team Member
4	Ayesha Abbas	Incident Response Team Member
5	Ahmed Raza	Incident Response Team Member
6	Sadia Khan	Recorder

4.3.1. IR Commander

Roles and Responsibilities:

- Oversee and prioritize actions during incident detection, analysis, and containment.
- Convey special requirements of high-severity incidents to the organization.
- Communicate potential impact to the CIO.
- Act as a liaison for all communications to and from the CIO.
- Assemble and lead the CSIRT.
- Ensure incident response personnel are trained and knowledgeable.
- Update and review the incident response plan and procedures.
- Act as the primary Incident Response Manager, declaring incidents and approving closure.

4.3.2. Incident Response Team Members (ConnectX)

Roles and Responsibilities:

- Assist in incident response as requested, with CSIRT duties taking priority.
- Understand ConnectX's incident response plan and procedures.
- Develop skills for incident response management continually.
- Ensure tools are configured to alert on security incidents.
- Analyze network traffic for signs of attacks.
- Review log files of critical systems for unusual activity.
- Monitor business applications and services for signs of attack.
- Collect incident information as requested by the IR Commander.
- Ensure evidence gathering and preservation are appropriate.
- Participate in tests of the incident response plan and procedures.

4.3.3. Recorder (ConnectX)

Roles and Responsibilities:

Begin formal documentation of the incident as assigned by the Incident Response Manager.

5. Incident Reporting Guide

Incident Type	Reporting Method	Available To	Anonymous	Response Time	Additional Information
Unauthorized Account Access	ConnectX Customer Support Portal	Customers	Yes	1 business day	Report any unauthorized access to mobile service accounts immediately.
Mobile Network Service Disruption	ConnectX Network Operations Center	Customers & Employees	No	Immediate during office hours. Otherwise within 1 hour of open.	Report disruptions in mobile network services promptly.
Billing Discrepancy	ConnectX Billing Support	Customers	Yes	Up to 2 business days	Notify ConnectX Billing Support for any billing-related issues.
Lost or Stolen SIM Card	ConnectX Customer Support Portal	Customers & Employees	Yes	Immediate	Report lost or stolen SIM cards promptly for security measures.
Phishing Attempt on Employees	ConnectX IT Help Desk	Employees	No	Immediate during office hours. Otherwise within 2 hours of open.	Report any phishing attempts targeting ConnectX employees.
Service Plan Modification Request	ConnectX Customer Support Portal	Customers	Yes	Up to 1 business day	Request changes to mobile service plans through the support portal.
Physical Theft of Equipment	ConnectX Security Team	Employees	No	Immediate	Report any physical theft of equipment immediately.
Unauthorized Access to Customer Data	ConnectX Data Security Team	Customers	Yes	Immediate during office hours. Otherwise within 1 hour of open.	Report any unauthorized access to customer data promptly.

Mobile Service Interruption during Peak Hours	ConnectX Network Operations Center	Customers	No	Immediate during office hours. Otherwise within 1 hour of open.	Report disruptions in mobile services during peak hours.
Suspicious Account Activity	ConnectX Customer Support Portal	Customers	Yes	Up to 1 business day	Report any suspicious activity related to mobile service accounts.
Service Plan Billing Error	ConnectX Billing Support	Customers	Yes	Up to 2 business days	Notify ConnectX Billing Support for any errors in service plan billing.
Mobile App Malfunction	ConnectX App Support	Customers & Employees	Yes	Up to 1 business day	Notify ConnectX App Support for issues with the mobile application.
Unauthorized Mobile Package Activation	ConnectX Customer Support Portal	Customers	Yes	Up to 1 business day	Report any unauthorized activation of mobile packages immediately.
Employee Mobile Device Policy Violation	ConnectX HR Department	Employees	No	Immediate during office hours. Otherwise within 2 hours of open.	Report any violations of the mobile device usage policy by employees.
Service Plan Upgrade/Downgrade Request	ConnectX Customer Support Portal	Customers	Yes	Up to 1 business day	Request upgrades or downgrades to mobile service plans through the portal.
Data Roaming Billing Error	ConnectX Billing Support	Customers	Yes	Up to 2 business days	Report any errors in data roaming charges to ConnectX Billing Support.

Mobile Device Connectivity Issues	ConnectX Network Operations Center	Customers & Employees	Yes	Up to 1 business day	Notify ConnectX of any connectivity issues with mobile devices.
Data Usage Discrepancy	ConnectX Billing Support	Customers	Yes	Up to 2 business days	Report any discrepancies in mobile data usage to ConnectX Billing Support.
Service Plan Cancellation Request	ConnectX Customer Support Portal	Customers	Yes	Up to 1 business day	Request cancellations of mobile service plans through the support portal.
Mobile Device Roaming Activation Issue	ConnectX Customer Support Portal	Customers	Yes	Up to 1 business day	Report any issues with the activation of mobile roaming services.
Network Speed Complaints	ConnectX Network Operations Center	Customers	Yes	Up to 2 business days	Report complaints related to network speed to ConnectX Network Operations.

6. Identification and Assessment

6.1.Identification

When a ConnectX employee or external party notices a suspicious anomaly in data, a system, or the network, or when a system alert generates an event, the Security Operations, Help Desk, or CSIRT must perform an initial investigation and verification of the event.

Events versus Incidents

As defined above, Events are observed changes in the normal behaviour of the system, environment, process, workflow, or personnel. Incidents are events that indicate a compromise of security or non-compliance with ConnectX's policy that negatively impacts (or may negatively impact) the organization.

To facilitate the task of identification of an incident, the following is a list of typical symptoms of security incidents for ConnectX:

a. Email or phone notification from an intrusion detection tool.
b. Suspicious entries in system or network accounting, or logs.
c. Discrepancies between logs.
d. Repetitive unsuccessful logon attempts within a short time interval.

e. Unexplained new user accounts.
f. Unexplained new files or unfamiliar file names.
g. Unexplained modifications to file lengths and/or dates, especially in system files.
h. Unexplained attempts to write to system files or changes in system files.
i. Unexplained modification or deletion of data.
j. Denial/disruption of service or inability of one or more users to log in to an account.
k. System crashes.
l. Poor system performance of dedicated servers.
m. Operation of a program or sniffer device used to capture network traffic.
n. Unusual time of usage (e.g., users log in during unusual times)
o. Unusual system resource consumption. (High CPU usage)
p. Last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
q. Unusual usage patterns (e.g., a user account associated with a user in Finance is being used to log in to an HR database).
r. Unauthorized changes to user permission or access.

Although there is no single symptom to conclusively prove that a security incident has taken place, observing one or more of these symptoms should prompt an observer to investigate more closely. Do not spend too much time with the initial identification of an incident as this will be further qualified in the containment phase.

NOTE: Compromised systems should be disconnected from the network rather than powered off. Powering off a compromised system could lead to loss of data, information or evidence required for a forensic investigation later. ONLY power off the system if it cannot be disconnected from the wired and wireless networks completely.

6.2. Assessment

Once a potential incident has been identified, part or all the CSIRT will be activated by the IR Commander to investigate the situation. The assessment will determine the category, scope, and potential impact of the incident.

6.2.1. Incident Categorization

The MITRE ATT&CK Framework is a globally accessible knowledge base of adversary tactics and techniques and should be leveraged when categorizing security incidents for ConnectX. While many techniques may be used in a single incident, select the method that was primarily leveraged by the adversary. Some examples of this may be:

- Phishing
- Unsecured Credentials
- Network Sniffing
- Man-in-the-Middle.
- Data Destruction
- OS Credential Dumping
- Event Triggered Execution
- Account Creation
- Disk Wipe
- Network Denial of Service

- Resource Hijacking
- Defacement
- File and Directory Permissions Modification

It should be noted that the MITRE ATT&CK Framework may not address some situations, specifically those without malicious intent, which trigger the Incident Response Management Plan. The following exceptions may require categories of their own as dictated by the organization's Risk Management entities or policies:

- Network Disruptions:
  - Description: Incidents affecting the availability and performance of the mobile network.
  - Examples: DDoS attacks, infrastructure failures.
- Data Breaches:
  - Description: Unauthorized access or disclosure of sensitive customer information.
  - Examples: Unauthorized access to customer databases, data leaks.
- Unauthorized Access:
  - Description: Unapproved access to systems, networks, or customer accounts.
  - Examples: Unauthorized login attempts, compromised credentials.
- Billing Irregularities:
  - Description: Anomalies in customer billing or fraudulent activities.
  - Examples: Billing errors, unauthorized charges.
- Physical Security Incidents:
  - Description: Events compromising the physical security of assets or infrastructure.
  - Examples: Break-ins, vandalism.
- Mobile App Issues:
  - Description: Malfunctions or security issues with mobile applications.
  - Examples: App crashes, vulnerabilities.
- Data Loss:
  - Description: Unintended or unauthorized loss of organizational data.
  - Examples: Accidental deletion, data corruption.
- Administrative Errors:
  - Description: Mistakes in administrative actions leading to security incidents.
  - Examples: Misconfigurations, accidental system changes.
- Unsecured Credentials:
  - Description: Compromised or exposed login credentials.
  - Examples: Stolen passwords, weak authentication mechanisms.
- Data Destruction:
  - Description: Intentional or unintentional destruction of critical data.
  - Examples: Malicious deletion, accidental data wipe.
- Lax File and Directory Permissions:
  - Description: Weak or misconfigured file and directory access controls.
  - Examples: Inadequate permission settings, unauthorized access.
- Account Creation:
  - Description: Unauthorized or suspicious creation of user accounts.

- Examples: Fake accounts, unauthorized user registration.

- Disk Wipe:
  - Description: Intentional removal or wiping of data from storage devices.
  - Examples: Secure data erasure, malicious disk wiping.
- Network Denial of Service:
  - Description: Deliberate disruption of network services to users.
  - Examples: DDoS attacks, network congestion.
- Resource Misuse (non-malicious):
  - Description: Inappropriate or unintended use of organizational resources.
  - Examples: Excessive bandwidth consumption, non-compliance with usage policies.

6.2.2. Incident Scope

Determining the scope will help the CSIRT understand the potential business impact of the incident. The following are some of the factors to consider when determining the scope:

1. How many systems are affected by this incident?
2. Is Confidential or Protected information involved?
3. What is/was the entry point for the incident (e.g., Internet, network, physical)?
4. What is the potential damage caused by the incident?
5. What is the estimated time to recover from the incident?
6. What resources are required to manage the situation?
7. How could the assessment be performed most effectively?

6.2.3. Incident Impact

Once the categorization and scope of an incident have been determined, the potential impact of the incident must be agreed upon. The severity of the incident will dictate the course of action to be taken to provide a resolution; however, in all instances, an incident report must be completed and reviewed by the Incident Response Commander. Functional and informational impacts are defined with initial response activity below:

Informational Impact	**Definition**	**CSIRT Response**
None	No information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	No action required.
Limited	Public or non-sensitive data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the data owners to determine the appropriate course of action.
Moderate	Internal information was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the CIO and IHT. CIO will work with management, legal, and data owners to determine the appropriate course of action.
Critical	Protected Data was accessed, exfiltrated, changed, deleted, or otherwise compromised.	Notify the CIO and IHT. CIO will work with legal to determine whether

		reportable, and the appropriate notification requirements.

Functional Impact	**Definition**	**CSIRT Response**
None	No effect on the organization's ability to provide all services to all users.	Create ticket and assign for remediation.
Limited	Minimal effect: the organization can still provide all critical services to all users but has lost efficiency.	Create ticket and assign for remediation, notify the CIO and IHT.
Moderate	The organization has lost the ability to provide a critical service to a subset of system users.	Initiate full CSIRT, involve the CIO and IHT.
Critical	The organization is no longer able to provide some critical services to any user.	Initiate full CSIRT, CIO, and IHT. Consider activation of the Disaster Recovery Plan.

Contact Information:

Category	Contact Person	Contact Details
High	Ali Khan	ali.khan@email.com
Medium	Fatima Ahmed	fatima.ahmed@email.com
Low	Saad Malik	saad.malik@email.com

7. Containment and Intelligence

Containment Strategies

ConnectX Technologies, a prominent mobile service provider, has defined robust containment strategies to address various incident types:

Stolen Credentials

In the event of stolen credentials, ConnectX will take decisive actions, including disabling compromised account credentials, resetting all active connections, reviewing user activity, reversing unauthorized changes, increasing alerting mechanisms, and implementing measures to harden against future attacks.

Ransomware

For ransomware incidents, ConnectX's approach involves isolating the impacted system, validating the ransomware claim, promptly contacting the insurance carrier, identifying additional impacted systems, and isolating them, as necessary.

DOS/DDOS

In the case of a Denial of Service (DOS) or Distributed Denial of Service (DDOS) attack, ConnectX will focus on controlling the Wide Area Network (WAN) and Internet Service Provider (ISP) to mitigate the impact.

Virus Outbreak

For a virus outbreak, ConnectX's strategy includes containing the Local Area Network (LAN) and affected systems to prevent further spread.

Data Loss

In response to data loss incidents, ConnectX will review user activity thoroughly and implement data breach response procedures to minimize the impact.

Website Defacement

In the event of website defacement, ConnectX will promptly repair the site and fortify it against future attacks.

Compromised API

For incidents involving compromised APIs, ConnectX will review changes made, repair the affected API, and implement measures to prevent future attacks.

Common Containment Steps

ConnectX recognizes the importance of critical decision-making during containment, involving collaboration between the Incident Response Manager, the Incident Response Commander, and Executive Management. Considerations include:

- Enabling disposable administrative accounts for secure investigation.
- Assessing the impact on critical services and determining the duration of potential service disruptions.
- Notifying the Cyber insurance carrier promptly.
- Assessing the likelihood of legal investigations and preserving evidence accordingly.
- Evaluating the success and potential damage of containment steps.
- Deciding on the involvement of third-party resources.
- Considering the necessity of notifying interested parties.

Engage Resources

ConnectX's Computer Security Incident Response Team (CSIRT) has the option to engage resources based on the severity of the incident:

- In-house Investigation: Quick response with competency varying based on skills.
- Law Enforcement: Varies by area and agency, preserving evidence for legal proceedings.
- Private Forensic Specialist: Quick response with highly skilled individuals, often with law enforcement background.

Preservation of Evidence

ConnectX emphasizes the preservation of evidence integrity, utilizing the (Company) Chain of Custody form and following NIST SP 800-86 guidelines. Detailed logs are maintained for all evidence collected during the investigation.

Reduce Impact

To minimize impact, ConnectX takes swift actions such as disabling accounts, isolating compromised systems, avoiding changes to volatile state data, and preserving system states for further investigation or use as evidence.

Collect Data and Increase Activity Logging

ConnectX intensifies monitoring, packet capture, and logging on affected systems to gather data for investigation. This includes enabling full packet capture, reviewing logs, creating memory images, and taking forensic images of affected systems.

Conduct Research

ConnectX conducts comprehensive research by performing Internet searches, consulting third-party resources, and collaborating with IT insurance carriers to gather information on the incident.

Notify Interested Parties

ConnectX assesses the need to notify both internal and external parties based on the incident's sensitivity, following the "need to know" principle and avoiding speculation in communications.

Key Decisions for Exiting Containment Phase

ConnectX determines the exit criteria for the containment phase, ensuring effective control of the attacker's abilities, identification of affected systems, and the collection of volatile data for further analysis.

Investigation

The CSIRT at ConnectX acknowledges that investigation is an ongoing process, with phases of containment, eradication, and recovery being cyclical. The focus is on fully identifying impacted systems, services, and data, including root cause analysis.

Initial Cause (“Root Cause”) Investigation

ConnectX conducts a thorough investigation into the initial cause or root cause of the incident, ideally concluding this phase before leaving the Eradication phase. Delays or modifications to the scope of investigation activities require approval from the Incident Response Commander.

The investigation involves various techniques, including interviews, capturing images and snapshots, obtaining relevant documents, observations, log analysis, anomaly detection, and behavioural monitoring.

ConnectX emphasizes the need to contract third-party experts if the investigation extends beyond the CSIRT's skills, involves systems owned by Cloud Service Providers, or requires in-depth forensic analysis. The goal is to ensure a comprehensive understanding of the incident and its implications.

This incident response plan aligns ConnectX Technologies with industry best practices, ensuring a systematic and thorough approach to handling security incidents.

Contact Information:

Level	Contact Person	Contact Details
Level 1	Ahmed Hassan	ahmed.hassan@email.com
Level 2	Aisha Shah	aisha.shah@email.com
Level 3	Farhan Khan	farhan.khan@email.com

8. Eradication

Eradication Strategies

ConnectX Technologies, in its commitment to cybersecurity, has defined comprehensive strategies to eradicate components of security incidents. These steps are crucial to eliminate the impact and prevent the recurrence of security breaches.

Administrative Tools

ConnectX emphasizes the use of separate administrative tools, such as boot disks, to investigate compromised hosts, considering the possibility of altered versions of original tools.

Eradication Steps

- Disable Breached User Accounts:

Immediate deactivation of compromised user accounts to prevent further unauthorized access.

- Reset Active Sessions:

Clearing any active sessions associated with breached accounts to ensure complete logout.

- Identify and Mitigate Vulnerabilities:

Conduct a thorough analysis to identify vulnerabilities exploited by the attacker and implement necessary mitigations.

- Close Unnecessary Open Ports:

Closing unnecessary open ports to minimize potential points of unauthorized access.

- Increase Authentication Security Measures:

Implementation of Multi-Factor Authentication (MFA) and geolocation restrictions to enhance authentication security.

- Enhance Security Logging, Alerting, and Monitoring:

Strengthening logging mechanisms, alert configurations, and continuous monitoring to promptly detect and respond to any suspicious activity.

- Clean Installation of Operating Systems and Applications:

Reinstalling operating systems and applications following (Company) system build standards, including security patches, service disabling, anti-virus installation, and adherence to system configuration baselines.

- Reset All Account Passwords:

Changing all account passwords, including domain, user, and service accounts, to ensure a clean slate for secure access.

Key Decisions for Exiting Eradication Phase

ConnectX makes critical decisions before concluding the eradication phase:

Root Cause Identification:

Confirming the identification of the root cause and remediation of identified vulnerabilities.

- Reset of Impacted Accounts:

Ensuring the reset of all impacted accounts, including CSIRT burner credentials.

- Configuration to Eliminate Repeat Occurrence:

Verification that the network and systems are configured to prevent a recurrence.

- Absence of Repeat Events:

Ensuring there is no evidence of repeat events or incidents.

- Authorization Sign-off:

Obtaining sign-off from the IR Manager for limited-severity incidents or CIO for moderate and critical-severity incidents.

Contact Information:

Phase	Contact Person	Contact Details
Phase 1	Nida Ali	nida.ali@email.com
Phase 2	Bilal Ahmed	bilal.ahmed@email.com
Phase 3	Zainab Khan	zainab.khan@email.com

9. Recovery Details

ConnectX places a strong emphasis on validating the success of eradication before proceeding to the recovery phase. This involves thorough testing in a controlled environment to ensure functionality and security.

Recovery Steps

ConnectX implements the following steps during the recovery phase:

- Restore Systems from Clean Backup:

Utilize clean backups to restore systems to a state before the incident.

- Replace Corrupted Data:

Replace any corrupted data with clean backup versions.

- Restore Network Connections and Access Rules:

Reestablish network connections and access rules following secure configurations.

- Communication with Interested Parties:

Informing relevant stakeholders about changes related to increased security measures.

- Increase Monitoring Activities:

Implementing heightened network and system monitoring activities, whether short or long-term.

- Internal Communication/Reporting:

Enhancing internal communication and reporting mechanisms related to monitoring activities.

- Engaging Third-Party Support:

Considering the engagement of a third party for additional support in detecting or preventing future attacks.

Contact Information:

Stage	Contact Person	Contact Details
Initial	Usman Raza	usman.raza@email.com
Ongoing	Sadia Malik	sadia.malik@email.com
Final	Imran Ahmed	imran.ahmed@email.com

10. Lessons Learned

The follow-up phase includes reporting and post-incident analysis on the system(s) that were the target of the incident and other potentially vulnerable systems. The objective of this phase is continued improvement to applicable security operations, response capabilities, and procedures.

Documentation

All details related to the incident response process must be formally documented and filed for easy reference. The following items must be maintained, whenever possible:

- All system events (audit records, logs).
- All actions taken (including the date and time that an action is performed).
- All external conversations.
- Investigator Notes compiled.
- Any deviations from SOP and justifications.

An incident report, documenting the following will be written by the CSIRT at the end of the response exercise:

- A description of the exact sequence of events.
- The method of discovery.
- Preventative measures put in place.
- Assessment to determine whether recovery was sufficient and what other recommendations should be considered.

The objective of the report is to identify potential areas of improvement in the incident handling and reporting procedures. Hence, the review of the report by management should be documented, together with the lessons learned, to improve the identified areas and used as reference for future incidents.

Lessons Learned and Remediation

The CSIRT will meet with relevant parties (technical staff, management, vendors, security team, etc.) to discuss and incorporate lessons learned from the incident to mitigate the risk of future incidents. Based on understanding of the root cause, steps will be taken to strengthen and improve ConnectX information systems, policies, procedures, safeguards, and/or training as necessary. Where mitigations or proposed changes are rejected, a Risk Acceptance Process must be followed. Incidents should be analyzed to look for trends and corrective action should be considered where appropriate.

Lessons Learned discussion should cover:

• Review of discovery and handling of incident(s).

• How well staff and management performed and whether documented procedures were followed.

• Review of actions that slowed or hindered recovery efforts.

• Proposed improvements to future response and communication efforts.

• Recommendations to increase the speed of future detection and response efforts.

• Recommendations for long and short-term remediation efforts.

At the end of Lessons Learned meetings, some sort of remediation needs to occur, either resolving the issues, installing compensating controls, or at a minimum formally assessing and accepting the risk. Recommendations for long and short-term remediation efforts must be added into the overall treatment plan.

Updates to the incident response procedures should also be considered and incorporated where areas of improvement are found. Voluntary information sharing should occur whenever possible with external stakeholders to achieve broader cybersecurity situational awareness (InfraGard, ISAC, etc.). Legal and Management must be consulted before doing so if a formal Information Sharing policy and process do not exist.

Forensic Analysis & Data Retention

In the event of possible legal action, forensic analysis will ensue in such manner as to preserve digital evidence consistent with legislative and legal requirements. Outside legal counsel and forensic experts may be required.

Forensic Investigator	Email
Muhammad Ali Khan	muhammad.ali@example.com
Ahmed Khan	ahmed.khan@example.com
Ayesha Malik	ayesha.malik@example.com
Farah Abbasi	farah.abbasi@example.com
Usman Raza	usman.raza@example.com

Consider the following when deciding whether and for how long to retain evidence related to the incident:

- Prosecution – is it likely that the attacker will be prosecuted? If so, evidence may need to be retained for multiple years.
- Reoccurrence – consider whether the evidence collected may be useful in case the attacker or a similar attack should occur in the future.
- Data Retention Policies – Consider the contents of evidence held (such as a system image capture) and retention policies related to this data (e.g., email retention policy).
- General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years.
- Cost – Depending on the type and amount of data or equipment preserved as evidence, cost may be a limiting factor.

Case 01:

1. Incident Identification

- Date/Time of Identification: November 15, 2023, 10:30 AM Identified By: Security Operations Center (SOC) automated alerting system Initial Symptoms:
- **Unauthorized access to customer databases detected**.
- Unusual network traffic patterns observed.
- Security alerts triggered by intrusion detection systems.

2. Immediate Actions

Containment:

- Disconnect affected systems:
- Identify affected servers: Database Server A, Database Server B.
- Isolate affected servers from the network.
- Use firewalls to block suspicious outbound traffic.

Reset passwords and credentials:

- Force password resets for all user accounts.
- Implement a temporary lockdown on all accounts until password changes are completed.
- Monitor and log all password reset activities.

Preservation of Evidence:

Initiate logging:

Enable detailed logging on affected systems and network devices.

Ensure logs capture timestamps, source IP addresses, and affected accounts.

Centralize logs to a secure, tamper-evident repository.

Forensic Analysis Preparation:

Follow NIST SP 800-86 guidelines for forensic evidence preservation.

Take snapshots of affected systems for offline forensic analysis.

Hash and timestamp all preserved evidence.

3. Incident Categorization

- Category: Data Breach MITRE ATT&CK Framework Reference:
- Tactic: Credential Access
- Technique: Exploitation of Valid Accounts (T1110)

4. Notification

Internal Notification:

- IR Commander: Sara Ahmed, sara.ahmed@connectx.com
- CIO: Hasan Khan, hasan.khan@connectx.com
- CSIRT: Security Team Distribution List
- Legal and Communications Departments: Legal Team Distribution List, comms@connectx.com
- External Notification: Prepare a statement for customers, advising them of the breach and potential impact.

Notify regulatory bodies as required by law.

5. Assessment and Impact Analysis

Scope of Breach:

- Number of affected accounts: 50,000
- Type of data accessed: Customer names, contact details, and encrypted passwords.
- Impact Analysis:
- Assess the potential harm to customers.
- Evaluate the impact on company reputation and trust.

6. Investigation

Root Cause Analysis:

- Conduct a thorough investigation to determine the root cause of the breach.
- Involve third-party cybersecurity experts if necessary.
- Identify Security Gaps:
- Review current security measures and identify any weaknesses that were exploited.

7. Eradication and Recovery

Eradication:

Patch vulnerabilities:

- Identify and prioritize vulnerabilities that were exploited.
- Apply security patches to affected systems promptly.
- Conduct regular vulnerability assessments.

Strengthen security protocols:

- Review and update firewall rules to prevent similar unauthorized access.
- Enhance intrusion detection and prevention systems.
- Implement network segmentation for sensitive data.

Multi-Factor Authentication (MFA):

- Enforce MFA for all user accounts.
- Implement adaptive authentication based on risk assessments.
- Conduct regular access reviews.

Recovery:

- Restore systems from clean backups:
- Validate the integrity of backups before restoration.
- Use incremental backups to minimize data loss.
- Monitor restored systems for any signs of compromise.

Enhanced Monitoring:

- Implement continuous monitoring for suspicious activities.
- Deploy Security Information and Event Management (SIEM) solutions.
- Configure alerts for anomalous behaviour and potential threats.

8. Communication

Internal Communication:

- Keep staff informed about the incident and recovery efforts.
- Provide guidelines on how to handle customer queries.

External Communication:

- Release a public statement with details about the breach, its impact, and the steps taken by ConnectX.
- Offer support and assistance to affected customers, such as credit monitoring services.

9. Forensic Analysis and Legal Considerations

Forensic Analysis:

Engage with forensic experts to conduct an in-depth analysis of the breach.

Legal and Compliance:

Consult with legal counsel for potential legal actions and compliance issues.

Determine the necessity and duration for retaining evidence as per legal advice and data retention policies.

10. Lesson Learned

Technical Improvements:

- Enhance network monitoring and anomaly detection capabilities.

- Implement machine learning algorithms for more advanced threat detection.
- Explore the use of behavioural analytics to identify abnormal user behaviour.
- Consider integrating threat intelligence feeds to enhance detection capabilities.
- Establish a dedicated incident response team with specialized training.
- Ensure incident response team members are certified in relevant cybersecurity disciplines.
- Provide regular training sessions and simulations to keep the team updated on the latest threats and response techniques.
- Consider cross-training team members to enhance skill diversity within the team.
- Regularly update and test incident response playbooks.
- Conduct tabletop exercises to validate and refine incident response procedures.
- Include scenario-based training that reflects emerging threat vectors.
- Collaborate with external cybersecurity experts to perform red teaming exercises.

Employee Training:

- Conduct regular cybersecurity awareness training for all employees.
- Integrate real-world case studies and examples into training materials.
- Emphasize the importance of reporting any suspicious activities promptly.
- Provide resources for employees to stay informed about current cyber threats.
- Simulate phishing attacks to test employee resilience.
- Conduct phishing drills with varying levels of complexity.
- Use results to tailor future training and awareness programs.
- Reward employees who demonstrate exemplary cybersecurity practices.
- Reinforce the importance of reporting security incidents promptly.
- Establish a clear reporting process for employees to follow.
- Communicate the role of reporting in preventing and mitigating security incidents.
- Encourage a culture of transparency and shared responsibility for security.

Third-Party Assessments:

- Implement regular third-party security assessments and penetration testing.
- Engage external security firms to perform comprehensive penetration tests.
- Ensure assessments cover both internal and external attack surfaces.
- Establish a recurring schedule for assessments based on risk assessments.
- Review and update vendor security requirements.
- Regularly assess and update security requirements for vendors.
- Consider implementing a continuous monitoring program for critical vendors.
- Collaborate with vendors to ensure mutual understanding of security expectations.

Case 02 Unauthorized System Access

Incident Identification:

Date/Time of Identification: November 20, 2023, 3:45 PM

Identified By: Network Monitoring System

Initial Symptoms:

- Unusual login attempts detected.

- Abnormal data exfiltration patterns observed.
- Anomalies in system resource usage.

Immediate Actions: Upon identification of the unauthorized system access incident, immediate containment measures were initiated. The affected systems, namely the Web Server and User Data, were promptly identified and isolated from the network. Temporary firewalls were deployed to block suspicious outbound traffic. Simultaneously, a comprehensive password reset initiative was enforced for all user accounts. To ensure security, a temporary lockdown was imposed on all accounts until the password changes were completed. Additionally, meticulous logging of all passwords reset activities was instituted.

Preservation of Evidence: Recognizing the critical importance of preserving evidence, detailed logging was enabled on the affected systems and network devices. This included capturing timestamps, source IP addresses, and details of affected accounts. To maintain the integrity of evidence, all logs were centralized into a secure and tamper-evident repository. As part of forensic analysis preparation, guidelines from NIST SP 800-86 were adhered to, involving the creation of snapshots of affected systems for subsequent offline forensic analysis. Hashing and timestamping were applied to all preserved evidence to facilitate a thorough investigation.

Incident Categorization: The incident was categorized as "Unauthorized System Access" with a specific MITRE ATT&CK Framework reference. The chosen tactic for this incident was "Initial Access," and the corresponding technique identified was "External Remote Services (T1133)."

Notification: Internal notification procedures were promptly activated, ensuring key stakeholders were informed. The Incident Response (IR) Commander, Sara Ahmed, and the Chief Information Officer (CIO), Hasan Khan, were notified. The ConnectX Security Incident Response Team (CSIRT) and relevant departments, including Legal and Communications, were also alerted. Externally, preparations were made to release a public statement to customers, apprising them of the breach and potential impact. Concurrently, regulatory bodies were notified as required by legal obligations.

Assessment and Impact Analysis: A thorough assessment of the incident's scope revealed that approximately 50,000 accounts were affected, compromising customer names, contact details, and encrypted passwords. The impact analysis encompassed an evaluation of potential harm to customers and the assessment of reputational damage and trust implications for ConnectX.

Investigation: Root cause analysis became a focal point of the investigation, aiming to determine how the unauthorized system access occurred. Third-party cybersecurity experts were engaged to ensure a comprehensive and unbiased assessment. The investigation further aimed to identify security gaps by reviewing current security measures and addressing weaknesses that may have been exploited.

Eradication and Recovery: The eradication phase focused on patching vulnerabilities promptly, prioritizing those exploited during the incident. Strengthening security protocols, including firewall rule reviews, enhancement of intrusion detection and prevention systems, and the implementation of network segmentation for sensitive data, became critical. Multi-Factor Authentication (MFA) was enforced for all user accounts, accompanied by adaptive

authentication based on risk assessments. Systems were restored from clean backups, validated for integrity, and continuously monitored for signs of compromise.

Communication: Both internal and external communications were orchestrated. Internally, staff were kept informed about the incident and ongoing recovery efforts. Guidelines for handling customer queries were provided. Externally, a public statement was released detailing the breach, its impact, and the steps taken by ConnectX. Support measures for affected customers, such as credit monitoring services, were included in the external communication strategy.

Forensic Analysis and Legal Considerations: Forensic analysis, conducted by engaged experts, delved into an in-depth examination of the breach. Legal counsel was consulted for potential legal actions and compliance issues. Decisions regarding the necessity and duration of retaining evidence were made in accordance with legal advice and data retention policies.

Lesson Learned: The incident prompted a comprehensive review of technical improvements, employee training initiatives, and third-party assessments. Technical enhancements included the implementation of advanced threat detection mechanisms, the exploration of behavioural analytics, and the integration of threat intelligence feeds. Employee training strategies emphasized real-world case studies, phishing simulations, and a culture of transparency and shared responsibility. Regular third-party security assessments and penetration testing were instituted to ensure a proactive security posture.

Case 03: Malicious Software Infection

Incident Identification:

Date/Time of Identification: December 5, 2023, 8:15 AM

Identified By: Endpoint Security System

Initial Symptoms:

- Unusual network behaviour observed.
- Increase in data exfiltration attempts.
- Anomalous activities reported by endpoint protection tools.

Immediate Actions: Upon identifying a malicious software infection, swift containment measures were initiated. Affected endpoints were immediately isolated from the network to prevent further propagation of the malware. Simultaneously, firewall rules were adjusted to block any communication attempts with known malicious domains. Recognizing the potential compromise of user credentials, password resets were enforced for all accounts suspected of exposure. Detailed logging was activated on both affected systems and endpoints, capturing essential information for subsequent forensic analysis.

Preservation of Evidence: To ensure a comprehensive forensic investigation, detailed logging on affected systems and endpoints was prioritized. This included capturing timestamps, source IP addresses, and specific details of the observed malicious activities. All logs were centralized into a secure, tamper-evident repository, adhering to NIST SP 800-86 guidelines. Snapshots of

affected systems were taken for offline forensic analysis, and each piece of preserved evidence was hashed and timestamped for integrity verification.

Incident Categorization: The incident was categorized as a "Malicious Software Infection" with a specific MITRE ATT&CK Framework reference. The identified tactic was "Execution" with the corresponding technique being "Malicious Code (T1034)."

Notification: Internal notification procedures were activated promptly. Key stakeholders, including the Incident Response (IR) Commander, Sara Ahmed, and the Chief Information Officer (CIO), Hasan Khan, were notified. The ConnectX Security Incident Response Team (CSIRT) and relevant departments, including Legal and Communications, were immediately alerted. Externally, a proactive strategy was formulated to prepare a public statement for customers, outlining the nature of the infection and recommended security measures. Regulatory bodies were notified in compliance with legal obligations.

Assessment and Impact Analysis: A thorough assessment revealed that a significant number of endpoints were compromised. The impact analysis included evaluating potential data exfiltration and the extent of system vulnerabilities. ConnectX prioritized understanding the malware's sophistication to gauge the potential harm to data integrity and confidentiality.

Investigation: Root cause analysis became a pivotal aspect of the investigation. External cybersecurity experts were engaged to conduct an in-depth analysis of the malware, its entry points, and the tactics employed for propagation. The investigation aimed to identify security gaps that allowed the malware to infiltrate the network.

Eradication and Recovery (Technical Measures):

Endpoint Remediation:

Employ advanced endpoint protection tools to scan and clean affected systems.

Isolate infected endpoints from the network to prevent lateral movement.

Conduct a thorough review of system logs to identify the initial point of compromise.

Network Sanitization:

Perform a comprehensive network-wide scan to identify and remove any remnants of the malware.

Adjust firewall rules to block known malicious domains and IPs.

Conduct penetration testing to identify potential hidden backdoors.

User Account Verification:

Implement multi-factor authentication (MFA) for all user accounts.

Conduct a detailed review of user account permissions and access levels.

Monitor and log all user account activities to identify any abnormal behaviour.

Patch Management:

Identify and apply security patches to vulnerable software and systems.

Implement a robust patch management system to ensure timely updates in the future.

Security Protocol Enhancement:

Enhance intrusion detection and prevention systems to recognize and mitigate similar threats.

Implement network segmentation to limit the lateral movement of malware.

Data Recovery:

Restore affected systems from clean and verified backups.

Validate the integrity of backups to ensure they are free from any traces of the malware.

Conduct incremental backups to minimize data loss.

Continuous Monitoring:

Implement continuous monitoring using Security Information and Event Management (SIEM) solutions.

Configure alerts for any suspicious activities or potential threats.

Conduct regular threat hunting exercises to proactively identify and neutralize emerging threats.

Incident Response Team Training:

Provide specialized training to incident response team members on handling sophisticated malware incidents.

Conduct tabletop exercises and simulations focusing on malware-related scenarios.

Communication: Internally, the incident response team maintained transparent communication with staff, providing updates on the incident and ongoing recovery efforts. Externally, a public statement was released outlining the incident, the steps taken for recovery, and recommendations for users to enhance their security posture.

Forensic Analysis and Legal Considerations: Engagement with forensic experts continued, aiming to uncover the full extent of the malware's impact. Legal counsel was consulted to assess potential legal actions, compliance issues, and adherence to data retention policies.

Lesson Learned: The incident prompted a series of technical improvements, including the deployment of more advanced endpoint protection tools, regular penetration testing, and enhanced network segmentation. Employee training programs were adapted to include specific modules on recognizing and reporting potential malware threats. Regular third-party assessments were implemented, covering both internal and external attack surfaces. The incident response playbook was updated, incorporating lessons learned from this specific malware infection incident.

Case 04: DDoS Attack and Service Disruption

Incident Identification:

Date/Time of Identification: January 10, 2024, 2:30 PM

Identified By: Network Operations Center (NOC)

Initial Symptoms:

- Sudden and significant increase in network traffic.
- Unavailability of critical online services.
- Degraded performance of web servers and applications.

Immediate Actions: Upon detecting the signs of a Distributed Denial of Service (DDoS) attack, ConnectX swiftly initiated a multifaceted response strategy. The Network Operations Center (NOC) took immediate steps to divert incoming traffic through DDoS mitigation services, leveraging advanced filtering mechanisms to analyse and block malicious IP addresses responsible for the attack. Simultaneously, adjustments were made to load balancer settings to efficiently distribute traffic and alleviate strain on the targeted servers. Recognizing the severity of the situation, the incident response team was promptly activated to coordinate the response efforts and communication strategies.

Notification: Internally, key stakeholders were promptly notified:

IR Commander: Sara Ahmed, sara.ahmed@connectx.com

CIO: Hasan Khan, hasan.khan@connectx.com

CSIRT: Security Team Distribution List Externally, a prepared statement for customers was readied, explaining the ongoing DDoS attack, its impact, and the steps being taken to restore services. Appropriate regulatory bodies were informed in adherence to legal requirements.

Preservation of Evidence: While the primary focus was on mitigating the ongoing DDoS attack, ConnectX prioritized the preservation of crucial evidence for subsequent analysis. Detailed logging of all incoming network traffic during the attack was initiated. Additionally, packet capture methods were employed to identify attack patterns and facilitate collaboration with DDoS mitigation service providers in retaining comprehensive logs.

Incident Categorization: The nature of the incident was categorized as a "DDoS Attack and Service Disruption," aligning with the MITRE ATT&CK Framework reference. The identified tactic was "Impact," and the specific technique was "Service Disruption (T1499)."

Assessment and Impact Analysis: Conducting a swift assessment, ConnectX gauged the scale of the DDoS attack and its direct impact on service availability. The attack's scale was unprecedented, with a significant volume surpassing normal traffic patterns. The consequence of the attack resulted in a temporary disruption of access to critical online services and a noticeable degradation in the performance of web servers and applications.

Investigation: Post-mitigation, ConnectX launched a comprehensive investigation to uncover the origin and tactics employed in the DDoS attack. Collaborative efforts with DDoS mitigation service providers were crucial in analysing attack vectors. Simultaneously, engagement with cybersecurity experts was initiated to identify vulnerabilities and potential entry points. The evaluation focused on understanding the effectiveness of existing DDoS mitigation measures.

Eradication and Recovery (Technical Measures):

- Network Infrastructure Strengthening: Enhancing the network infrastructure to withstand future DDoS attacks became a priority. Collaborative efforts with Internet Service Providers (ISPs) were undertaken to implement traffic filtering upstream, reinforcing the overall resilience of the network.
- DDoS Mitigation System Optimization: Continuous optimization of DDoS mitigation systems was pursued to ensure faster and more accurate identification of malicious traffic. Regular updates and testing of mitigation rules were implemented to adapt to evolving attack techniques effectively.
- Load Balancer Redundancy: The implementation of redundant load balancers became a key strategy to ensure effective traffic distribution during high-volume scenarios. Regular testing of load balancing configurations was conducted to guarantee seamless failover in case of an attack.
- Cloud-based Service Scaling: Leveraging cloud-based services to scale resources during peak traffic emerged as a proactive measure to prevent service disruption. The implementation of auto-scaling policies based on predefined thresholds became integral to maintaining service availability.
- Incident Response Team Training: Specialized training sessions for incident response team members were conducted to enhance their capabilities in DDoS attack detection and mitigation. Simulated scenarios of DDoS attacks were included in tabletop exercises to continuously refine response strategies.
- Communication: Internally, ConnectX maintained ongoing communication to keep stakeholders informed about the progress of DDoS attack mitigation and recovery efforts. Externally, a transparent and informative public statement was released, detailing the nature of the attack, the impact on services, and the proactive measures taken to prevent future disruptions.

Forensic Analysis and Legal Considerations: Collaboration with forensic experts continued to analyse the attack's forensic footprint. Collecting and analysing logs from affected systems and network devices remained a priority. Simultaneously, ConnectX closely collaborated with legal counsel to assess potential legal actions and compliance considerations.

Lesson Learned: The DDoS attack prompted a re-evaluation of network resilience and mitigation strategies. Technical improvements included the optimization of DDoS mitigation systems, enhancement of load balancing mechanisms, and the exploration of cloud-based scaling solutions. Continuous training and simulations for the incident response team were emphasized to ensure preparedness for future DDoS incidents. Regular collaboration with DDoS mitigation service providers and ISPs was established to stay ahead of emerging threats. The incident underscored the importance of proactive measures to mitigate the impact of DDoS attacks and reinforced the need for a robust incident response strategy.

Disaster Recovery Plan

Introduction

This Disaster Recovery Plan (DRP) serves as a foundational document for ConnectX, a leading Pakistani telecommunications company. It provides a comprehensive framework outlining ConnectX's preparedness and recovery procedures in the face of potential disasters. This plan serves as a critical resource, detailing the steps necessary for disaster recovery to ensure the uninterrupted functionality of essential operations.

Definition of a Disaster

At ConnectX, a disaster is defined as any event, whether triggered by nature or human actions, which disrupts the regular functions of the IT department. These events include:

Dysfunction of one or more vital systems.

Extended unavailability of the building, even if operational systems within it are intact.

Building availability but with non-functional systems.

Complete non-functionality of both the building and its systems.

ConnectX acknowledges various disaster-inducing events, such as:

- Fire
- Pandemics
- Power outages
- Civil unrest
- Theft
- Terrorism

Purpose

The purpose of this DRP is twofold: firstly, to compile pertinent information regarding ConnectX's ability to endure a disaster, and secondly, to document the step-by-step procedures that ConnectX will follow if a disaster occurs.

In the event of a disaster, ConnectX prioritizes human safety, ensuring the well-being of all employees and individuals on its premises before initiating any secondary measures. Following the assurance of safety, the goal is to implement the outlined steps in this DRP swiftly, aiming to restore all departments and groups to business-as-usual as promptly as possible.

This includes:

- Preventing the loss of organizational resources such as hardware, data, and physical IT assets.
- Minimizing downtime related to IT.
- Keeping the business running efficiently post-disaster.
- This DRP document also outlines how it will be maintained and regularly tested for effectiveness.

Scope

ConnectX's DRP takes into consideration the following areas:

- Network Infrastructure
- Servers Infrastructure
- Telephony System
- Data Storage and Backup Systems
- Data Output Devices
- End-user Computers
- Organizational Software Systems
- Database Systems
- IT Documentation

For disasters not covered in this document, reference ConnectX's business continuity plan or contact the Business Continuity Lead at [Business Continuity Lead Contact Information].

Version Information & Changes

Any modifications to the DRP will be documented in this section. The Disaster Recovery Lead is responsible for ensuring all copies of the DRP are up to date. Version numbers will indicate updates.

Name of Person Making Change	Role of Person Making Change	Date of Change	Version Number	Notes
Usman Shahid	DR Led	01/01/22	1.0	Initial version of DR Plan
Sarah Ahmed	DR Led	01/15/22	1.1	Updated contact information
Ahmed Khan	CEO	02/01/22	2.0	Revised disaster scenarios

Disaster Recovery Lead

Mandatory

The Disaster Recovery Lead is the key decision-maker responsible for guiding the entire recovery process. This individual's primary responsibilities include:

- Determining when a disaster has occurred and initiating the DRP.
- Activating the DR Call Tree to coordinate responses.
- Serving as the central point of contact and overseeing all DR teams.
- Organizing and leading regular meetings with DR Team leads.
- Presenting updates and decisions to the Management Team.
- Managing DRP tests and authoring updates.

Contact Information

Name	Role/Title	Work Phone	Home Phone

Ali Ahmed	Primary Disaster Lead	0333-1234567	0333-7654321
Hassan Raza	Secondary Disaster Lead	0333-2345678	0333-8765432
Fatima Khan	Disaster Management Team Lead	0333-3456789	0333-9876543
Muhammad Ali	Facilities Team Lead	0333-4567890	0333-1234567
Ayesha Siddiqui	Network Team Lead	0333-5678901	0333-2345678

Disaster Management Team

Elective

The Disaster Management Team oversees the recovery process, evaluates the disaster's impact, and ensures alignment with DRP policies. Responsibilities include:

- Setting the DRP in motion after the Disaster Recovery Lead's declaration.
- Assessing the magnitude and class of the disaster.
- Communicating the disaster to other recovery teams.
- Coordinating with other teams to restore business operations.
- Ensuring adherence to DRP and organizational policies.
- Getting the secondary site ready and ensuring functionality and security.
- Providing detailed reports on recovery steps.
- Summarizing costs and activities post-recovery.

Contact Information

Name	**Role/Title**	**Work Phone**	**Home Phone**
Ali Ahmed	Facilities Team Lead	0333-4567890	0333-1234567
Ayesha Kamran	Network Team Lead	0333-5678901	0333-2345678

Facilities Team

Mandatory

The Facilities Team manages physical facilities housing IT systems, ensuring standby facilities are operational, and overseeing repairs post-disaster. Responsibilities include:

- Maintaining the standby facility.
- Providing transportation, accommodation, and supplies for employees at the standby facility.
- Assessing physical damage to the primary facility.

- Collaborating with insurers in case of damage or losses.
- Coordinating resources for rebuilding or repairing facilities.
- Summarizing costs and activities post-recovery.

Contact Information

Name	**Role/Title**	**Work Phone**	**Home Phone**
Ali Ahmed	Disaster Management Team Lead	0333-3456789	0333-9876543
Hassan Raza	Facilities Team Lead	0333-4567890	0333-1234567
Fatima Khan	Network Team Lead	0333-5678901	0333-2345678

Network Team

Role & Responsibilities:

1. Identify non-functioning network services at the primary facility during a disaster.
2. Prioritize the recovery of services with minimal business impact.
3. Coordinate with third-party providers for connectivity restoration.
4. Activate network services at the secondary facility in case of migration.
5. Provide connectivity in order of priority: DR Teams, C-level staff, IT employees, other employees.
6. Implement necessary tools and systems at standby and primary facilities.
7. Prepare a detailed cost report post-disaster for the Disaster Recovery Lead.

Name	Role/Title	Work Phone	Home Phone
Ali Khan	Network Manager	03227117753	03227117753
Fatima Akhtar	Network Administrator	03227117753	03227117753

Server Team

Role & Responsibilities:

1. Identify non-functioning servers at the primary facility during a disaster.
2. Prioritize server recovery with least business impact.
3. Maintain updated patches and data copies for secondary servers.
4. Ensure compliance with company server policies.
5. Implement necessary hardware/tools at standby and primary facilities.
6. Compile cost summary post-disaster for the Disaster Recovery Lead.

Name	Role/Title	Work Phone	Home Phone
Hassan Ali	Operations Manager	03227117753	03227117753
Sana Riaz	Systems Administrator	03227117753	03227117753

Applications Team

Role & Responsibilities:

1. Identify non-functioning applications at the primary facility during a disaster.
2. Prioritize application recovery based on business impact.
3. Maintain updated patches for secondary servers.

4. Implement necessary software at standby and primary facilities.
5. Prepare cost report post-disaster for the Disaster Recovery Lead.

Name	Role/Title	Work Phone	Home Phone
Ayesha Ahmed	Program Manager	03227117753	03227117753
Usman Khan	Systems Administrator	03227117753	03227117753

Operations Team

Role & Responsibilities:

1. Provision employees with necessary tools during a disaster.
2. Manage supplies and equipment distribution.
3. Maintain a log of equipment usage.
4. Prepare a cost report post-disaster for the Disaster Recovery Lead.

Name	Role/Title	Work Phone	Home Phone
Farah Ali	Helpdesk Manager	03227117753	03227117753
Imran Khan	Systems Administrator	03227117753	03227117753

Senior Management Team

Role & Responsibilities:

1. Oversee and make critical business decisions related to disaster recovery.
2. Ensure accountability of the Disaster Recovery Team Lead.

Name	Role/Title	Work Phone	Home Phone
Omar Ahmed	CEO	03227117753	03227117753
Zara Khan	COO	03227117753	03227117753

Communication Team

Role & Responsibilities:

1. Communicate disaster impact to employees, partners, clients, vendors, and media.
2. Prepare a cost report post-disaster for the Disaster Recovery Lead.

Name	Role/Title	Work Phone	Home Phone
Ahmed Ali	VP HR	03227117753	03227117753
Sara Khan	Media Relations	03227117753	03227117753

Finance Team

Role & Responsibilities:

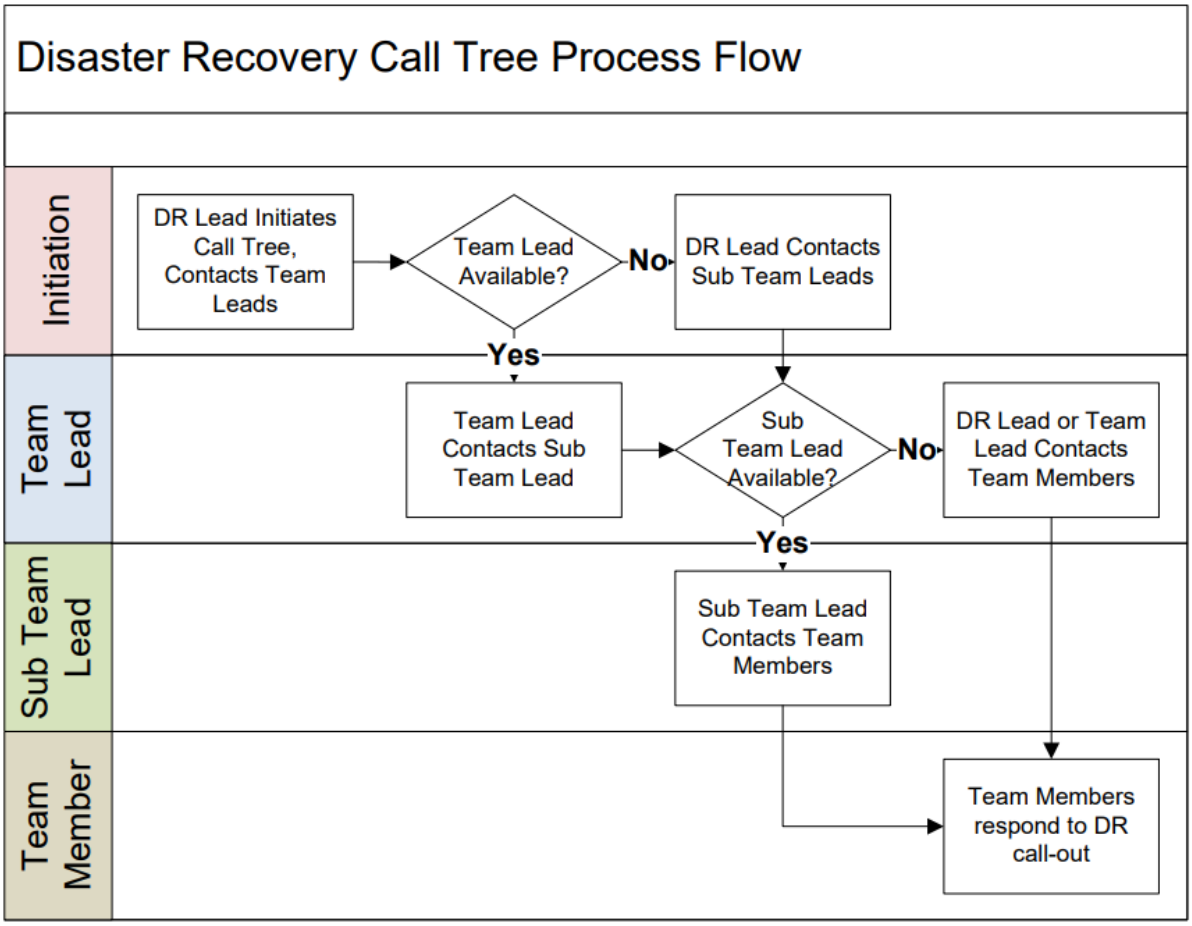
1. Ensure availability of funds for both disaster-related and day-to-day expenses.
2. Manage small-scale expenses caused by the disaster (accommodations, food for DR team, incremental bills).
3. Manage large-scale expenses (new equipment, facility repairs) by overseeing accessible credit.
4. Review and approve spending by Disaster Teams.
5. Facilitate normal payroll processes.
6. Coordinate with creditors for payment extensions.
7. Liaise with banking partners for any necessary replacements (checks, bank books) due to the disaster.

Name	Role/Title	Work Phone	Home Phone
Ali Khan	Finance Head	03227117753	03227117753
Fatima Ahmed	Financial Controller	03227117753	03227117753

Disaster Recovery Call Tree

Role/Position	Name	Contact (Office)	Contact (Mobile)	Contact (Home)
DR Led	Ali Khan	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
DR Management Team Lead	Fatima Ahmed	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- DR Management Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- DR Management Team 2	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
Facilities Team Lead	Hassan Ali	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- Facilities Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
Network Team Lead	Fatima Khan	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- LAN Team Led	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
-- LAN Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- WAN Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
-- WAN Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
Server Team Led	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- Server Type 1 Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
-- Server Type 1 Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- Server Type 2 Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
-- Server Type 2 Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
Applications Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- App 1 Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
-- App 1 Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX

- App 2 Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
-- App 2 Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
Management Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- Management Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
Communications Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- Communications Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
Finance Team Lead	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX
- Finance Team 1	[Name]	0333-XXXXXXX	0333-XXXXXXX	0333-XXXXXXX



Communicating During a Disaster

Communicating with the Authorities

The Communications Team will immediately notify the authorities with the following details:

Location: Main office building, Islamabad G8

Nature of Disaster: Fire outbreak

Magnitude: Significant structural damage, affecting multiple floors

Impact: Employee safety concerns, potential service disruptions

Assistance Required: Immediate firefighting support and structural safety assessment.

Anticipated Timelines: Initial assessment within the hour, ongoing updates

Authorities Contacts:

Authorities	Point of Contact	Phone Number	E-mail
Police Department	Asad Ali	0333-1234567	asad.ali@police.pk
Fire Department	Sara Khan	0333-7654321	sara.khan@firedept.pk

Communicating with Employees

The Communications Team will reach out to employees using the following communication channels prioritized as:

- Corporate e-mail
- Personal e-mail
- Home phone calls
- Mobile phone calls

Employees to Notify:

Name	Role/Title	Home Phone	Mobile Phone	Personal E-mail
Ali Ahmed	Manager	0333-9876543	0333-2345678	ali.ahmed@email.com
Hassan Raza	Executive	0333-1234567	0333-3456789	hassan.raza@email.com
Fatima Khan	Coordinator	0333-2345678	0333-4567890	fatima.khan@email.com

Information to Employees:

- Safety instructions
- Alternative work arrangements
- Available services and support’

Communicating with Clients

Clients will be informed of the potential impact on service offerings, delivery schedules, and data security. Crucial clients will be contacted first via e-mail, followed by a phone call for confirmation.

Crucial Clients:

Company Name	Point of Contact	Phone Number	Email
XYZ Corporation	Shahid Malik	0333-1111111	shahid.malik@xyzcorp.pk
ABC Enterprises	Ayesha Ali	0333-2222222	ayesha.ali@abcent.com.pk

Communicating with Vendors

Crucial Vendors

Crucial vendors will be informed about the disaster and its impact regarding service requirements, delivery locations, contact information adjustments, and anticipated timelines.

Crucial Vendors:

Company Name	Point of Contact	Phone Number	Email
XYZ Solutions	Ali Khan	0333-1111111	ali@xyzsolutions.com.pk
ABC Communications	Sara Ahmed	0333-2222222	sara@abccommunications.pk

Secondary Vendors

Secondary vendors will be contacted after crucial vendors have been informed. They will receive information about the disaster's impact and necessary adjustments.

Secondary Vendors:

Company Name	Point of Contact	Phone Number	Email
PQR Technologies	Asad Ali	0333-3333333	asad@pqrtech.com.pk
LMN Services	Ayesha Khan	0333-4444444	ayesha@lmnservices.pk

Communicating with the Media

Media Contacts

The Communications Team will inform the media about the disaster, providing official statements, details about the disaster's magnitude, impact, and anticipated timelines.

Media Contacts:

Company Name	Point of Contact	Phone Number	Email
The Daily Gazette	Kamran Khan	0333-5555555	kamran@gazette.pk
TechInsight Magazine	Sadia Ali	0333-6666666	sadia@techinsightmag.pk

Recovery Facilities

Mobile Site Recovery Plan

In the event of an incident requiring the activation of ConnectX's mobile site, a comprehensive recovery plan is essential. This plan outlines the technical and procedural steps to ensure a swift and effective response.

1. Notification Protocol:

Action: Immediately alert the Disaster Recovery Team Lead, Mr. Naveed Khurshid, at connectx.naveed@connectx.com, providing detailed incident information.

Role Description: Mr. Naveed Khurshid oversees the entire disaster recovery phase, prepares incident reports, and presents post-disaster analysis reports to the executive council.

2. Mobile Site Initiation:

Action: Notify the Mobile Site Initiation Department Head, Abdullah Khizar, at abdullah.khizar@connectx.com, within the first 24 hours of the disaster.

Formal Report: Submit a detailed report to Mobile Site Manager Abdullah Khizar within 24 hours, initializing operational sequences at the mobile site.

3. Backup Verification:

Action: Verify the integrity and availability of required backups for the mobile site.

Data Loading: Confirm the availability of all data needed to load mobile site backup devices for continuous business operations.

4. Equipment Procurement:

Action: Initiate procurement for backup equipment and issue a purchase order to ensure operational resilience.

5. Logistics and Communication:

Coordination: Coordinate with the Logistics Coordinator for strategic deployment of a trailer for the mobile site.

Communication Infrastructure: Notify the telephone company (e.g., ConnectX Jazz) of potential emergency line changes and coordinate adjustments promptly.

6. Infrastructure Establishment:

Action: Commence the establishment of power and communication infrastructure at the mobile site location.

Readiness Confirmation: Confirm readiness for immediate hookup upon the trailer's arrival.

7. Network Rerouting:

Action: Identify entry points of telephone lines into the building and reroute network lines from the primary to the mobile site.

Technical Team: Task the mobile site technical transfer team with redirecting lines to a secure area in case of a disaster.

8. System Activation:

Activation Process: While shifting through the trailer, connect to the power supply, conduct necessary checks, and ensure all systems are operational.

Data Loading: Load the system from verified backups and confirm successful data transfer.

9. Operational Resumption:

Tasks: Resume daily operational tasks, implement daily, weekly, and monthly save procedures.

Security Measures: Implement security measures to safeguard the mobile site.

Documentation: Maintain a detailed maintenance log for all activities.

ConnectX Hot Site Recovery Plan

1. Disaster Recovery Service Notification:

Action: Notify the Disaster Recovery Service promptly about the nature of the disaster and request the activation of a hot site for temporary operations.

2. Modems Air Shipment:

Coordination: Coordinate the air shipment of essential modems to the hot site to ensure seamless communication during the recovery process.

3. Written Confirmation:

Formal Communication: Confirm disaster details in writing to the disaster recovery service within 48 hours, providing formal documentation.

4. Travel Arrangements:

Initiation: Initiate and manage necessary travel arrangements for the operations team, ensuring timely arrival at the designated hot site.

5. Tapes Availability:

Verification: Confirm the availability and proper packing of required tapes essential for the restoration process at the hot site.

6. Purchase Order Preparation:

Financial Management: Prepare a purchase order covering the usage of the backup system at the hot site, managing financial aspects associated with the recovery.

7. Materials Checklist Review:

Verification: Review the materials checklist to ensure all necessary items are packed before the operations team departs for the hot site.

8. Information Sharing:

Communication: Provide essential information to the disaster recovery team at the hot site, facilitating the initiation of the restoration process.

9. Travel Expenses:

Responsibility: Ensure the provision of travel expenses, including necessary cash advances, for the operations team traveling to the hot site.

Site Rebuilding Process

Following a disaster, the reconstruction process for ConnectX's data center is meticulously designed, emphasizing the integration of cutting-edge technologies within a secure and optimized environment.

Floor Plan of Data Center:

Blueprint Utilization: Employ the existing floor plan as a foundational blueprint for the reconstruction process.

Innovative Layout: Incorporate advanced layouts and security features, aligning with the latest industry standards and best practices.

Hardware Needs Assessment:

Roles and Functions Analysis: Assess current hardware requirements based on the diverse roles and functions of the data center.

Technological Advancements: Explore alternative hardware solutions, aligning with the latest technological trends and ConnectX's infrastructure vision.

Infrastructure Specifications:

Data Center Size: maintain a data center with a total square footage of 100,000 square feet.

Power Requirements: ensure power availability ranging from 1 to 5 Mega Watts.

Security Requirements:

Locked Area: Maintain a secured, locked area for the data center.

Combination Lock: Install a combination lock on one door for additional security measures.

Infrastructure Features:

Enhanced Structural Integrity:

Floor-to-Ceiling Studding: Rebuild with floor-to-ceiling studding to enhance structural integrity and fortify against potential risks.

Detection Systems:

Temperature, Water, Smoke, Fire, and Motion Detectors: Integrate comprehensive detection systems to monitor and respond to high temperature, water leakage, smoke, fire, and unauthorized motion.

Floor Design:

Raised Floor: Maintain a raised floor design in the scenario to facilitate efficient cabling and airflow management, ensuring optimal performance.

Description of Recovery Facilities

The Disaster Command and Control Center or Standby facility will be used after the Disaster Recovery Lead has declared that a disaster has occurred. This location is a separate location from the primary facility. The current facility, located at 123 Main Street, Islamabad, is approximately 15 miles away from the primary facility.

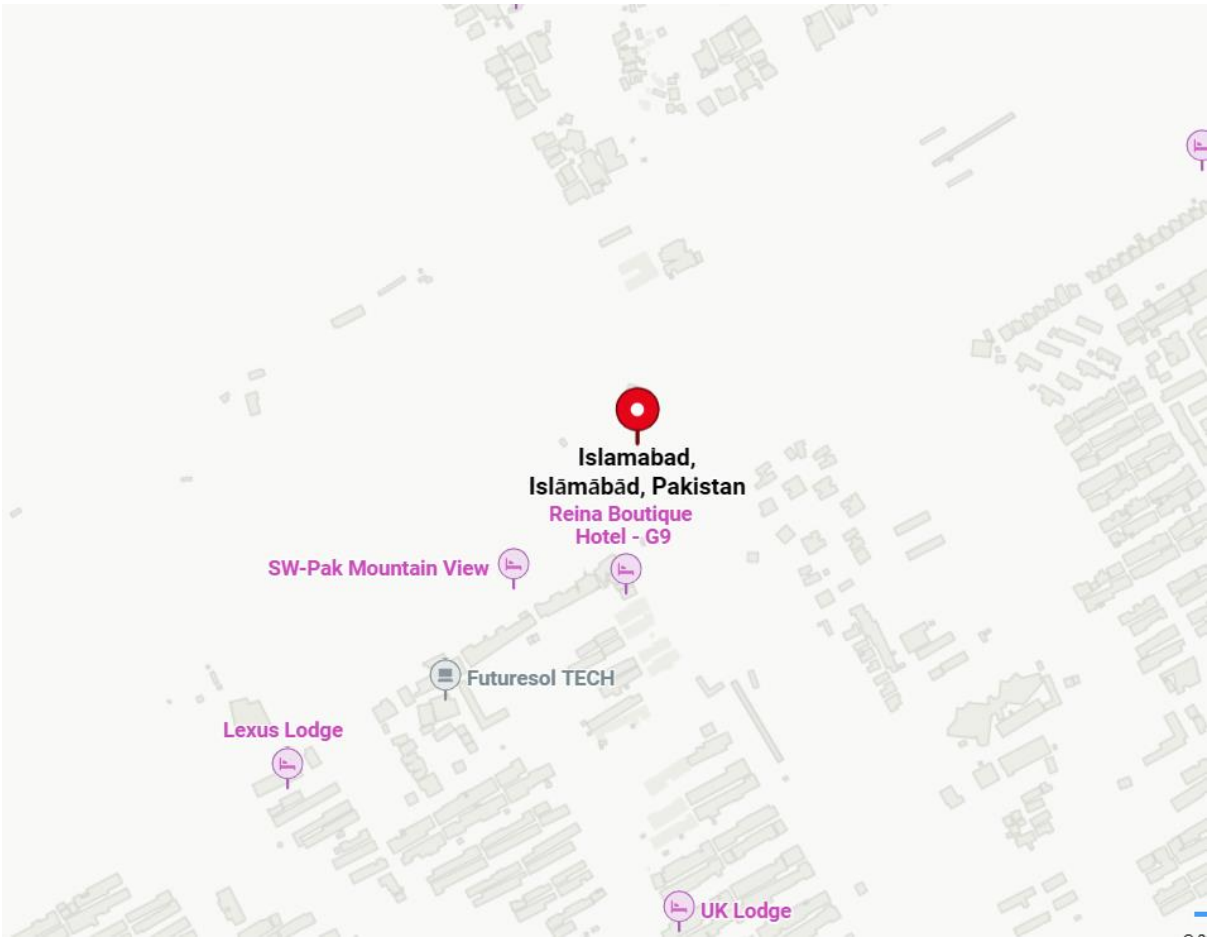
The standby facility will be used by the IT department and the Disaster Recovery teams; it will function as a central location where all decisions during the disaster will be made. It will also function as a communications hub for ConnectX.

The standby facility must always have the following resources available:

- Copies of this DRP document

- Fully redundant server room
- 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

Map of Standby Facility Location



Transportation to the Standby Facility

Taxi Providers:

Taxi Company	Address	Phone Number
Taxi Company 1	456 Taxi Street, Islamabad	+92 51 1234567
Taxi Company 2	789 Taxi Avenue, Islamabad	+92 51 7654321

Rental Car Providers:

Rental Car Company	Address	Phone Number
Rental Car Company 1	123 Car Rental Road, Islamabad	+92 51 9876543
Rental Car Company 2	321 Car Hire Street, Islamabad	+92 51 2345678

Travel Agents (for air or train travel):

Travel Agent	**Address**	**Phone Number**
Travel Agent 1	567 Travel Plaza, Islamabad	+92 51 8765432
Travel Agent 2	890 Travel Center, Islamabad	+92 51 8765432

a. Operational Considerations

If employees are required to stay at the Standby Facility for extended periods of time and require hotel accommodations, they will be provided by <>. The Facilities Team will be responsible for determining which employees require hotel accommodations and ensuring sufficient rooms are made availablee.

Accommodations:

Hotel Name	Address	Phone Number
Islamabad Grand	123 Luxe Avenue, Islamabad	+92 51 1234567
Pearl Palace	456 Comfort Street, Lahore	+92 42 7654321
Karachi Heights	789 Seaview Boulevard, Karachi	+92 21 9876543
Peshawar Plaza	101 Heritage Road, Peshawar	+92 91 8765432

Catering:

Caterer Name	Address	Phone Number
Tasty Treats	123 Catering Street, Islamabad	+92 51 1234567
Delightful Dining	456 Food Plaza, Lahore	+92 42 7654321

Standby Facility Maintenance:

Maintenance Company	Address	Phone Number
Facility Care Inc.	789 Maintenance Avenue, Karachi	+92 21 9876543

b. Data and Backups

This section explains where all the organization’s data resides as well as where it is backed up to. Use this information to locate and restore data in the event of a disaster.

Rank	Data Name or Group	Data Type	Backup Frequency	Backup Location(s)
1	Customer Billing Information	Personally, Identifying Information	Daily	Onsite Server, Offsite Data Center
2	Network Configuration Settings	Confidential	Weekly	Cloud Storage, Offsite Data Center
3	Employee Contact Information	Personally, Identifying Information	Daily	Onsite Server, Offsite Data Center

4	Call Records	Confidential	Hourly	Onsite Database, Offsite Data Center, Tape Backups
5	Marketing Campaign Data	Public	Monthly	Cloud Storage, Offsite Data Center
6	Network Performance Metrics	Confidential	Daily	Onsite Monitoring Server, Offsite Data Center
7	Product Development Documents	Confidential	Bi-weekly	Onsite Development Server, Offsite Data Center
8	Customer Support Tickets	Personally, Identifying Information	Hourly	Onsite Helpdesk Server, Offsite Data Center
9	Inventory and Stock Information	Confidential	Weekly	Onsite Database, Offsite Data Center, Cloud Storage
10	System Configuration Backups	Confidential	Daily	Onsite Server, Offsite Data Center, Cloud Storage
11	Financial Transactions	Personally, Identifying Information	Daily	Onsite Finance Server, Offsite Data Center, Tape Backups
12	Regulatory Compliance Reports	Confidential	Monthly	Onsite Server, Offsite Data Center
13	Mobile App User Data	Personally, Identifying Information	Hourly	Onsite App Servers, Offsite Data Center
14	HR Records	Personally, Identifying Information	Weekly	Onsite HR Server, Offsite Data Center
15	Social Media Analytics	Public	Daily	Cloud Storage, Offsite Data Center

Case 01:

Dealing with a Cybersecurity Breach:

In the event of a cybersecurity breach at ConnectX, the organization's response strategy is intricately designed to address the unique challenges posed by digital threats. The initiation of this comprehensive response plan is anchored in advanced threat detection mechanisms. ConnectX employs cutting-edge cybersecurity tools and monitoring systems that continuously assess network activity in real-time. These systems, integrated with intrusion detection and prevention systems, form the first line of defence in identifying unauthorized access and potential breaches.

Disaster Identification and Declaration:

Upon the identification of a cybersecurity breach, the Incident Response Lead promptly declares a state of disaster, triggering the activation of ConnectX's Cybersecurity-specific

Incident Response Plan. This plan is meticulously tailored to the organization's digital infrastructure, ensuring a swift and technical response. Key personnel, comprising the Incident Response Team, are immediately notified, and directed to their designated roles.

Communicating the Cybersecurity Breach:

The Communications Team, armed with a precise cybersecurity communication protocol, undertakes a critical role in notifying internal stakeholders and relevant authorities about the breach. Simultaneously, internal communication channels are activated to disseminate real-time updates to all employees, providing guidance on secure communication practices and steps to mitigate further risks.

Assessment of Current Damage and Prevention of Further Damage:

Following the confirmation of the cybersecurity breach, specialized incident response teams are deployed to conduct an in-depth assessment of the compromised systems. These teams, equipped with technical expertise, employ advanced forensics tools and methodologies to identify the extent of the breach, the compromised data, and potential vulnerabilities. Immediate measures are taken to contain the breach, prevent further unauthorized access, and secure critical systems.

In parallel, ConnectX focuses on preventing further damage to digital assets, incorporating technical strategies such as isolating compromised systems, enhancing network segmentation, and deploying patches to address identified vulnerabilities. This proactive approach aligns with the organization's commitment to minimizing the impact of the cybersecurity breach on its digital infrastructure.

Standby Facility Activation:

As the incident response teams work to contain and assess the cybersecurity breach, the designated standby facility for digital operations is activated to ensure the continuity of critical digital services. This involves a technical handover of essential systems and services to the standby digital facility, seamlessly transitioning digital operations.

Establish IT Operations:

ConnectX's IT and cybersecurity teams work swiftly to enhance security measures and restore affected systems at the standby digital facility. This process includes the deployment of cybersecurity enhancements, updates to security protocols, and the implementation of additional security layers to fortify digital defences. Advanced threat hunting and eradication processes are initiated to facilitate a seamless transition and uphold operational cybersecurity.

Repair and Restoration of Compromised Systems:

In the aftermath of the cybersecurity breach, ConnectX collaborates with relevant cybersecurity experts, forensic analysts, and authorities to initiate the repair and restoration of compromised systems. This technical evaluation informs the organization's strategy for strengthening cybersecurity postures, incorporating lessons learned from the breach to enhance future resilience. The restoration process is executed with precision, utilizing advanced cybersecurity measures and best practices.

Note: Regular cybersecurity training sessions, including simulated phishing attacks and incident response drills, are conducted to familiarize personnel with specific actions to be taken during digital security incidents. This plan ensures a more detailed and context-specific response to a cybersecurity breach disaster.

Plan Testing & Maintenance

Maintenance:

The ConnectX Disaster Recovery Plan (DRP) will be updated annually or any time a major system update or upgrade is performed, whichever is more frequent. The Disaster Recovery Lead is responsible for updating the entire document and may request information and updates from relevant employees and departments within the organization.

- Maintenance tasks will include, but are not limited to:
- Ensuring call trees are up to date.
- Verifying the accuracy of all team lists.
- Reviewing the plan to ensure instructions remain relevant to the organization.
- Making major changes and revisions to reflect organizational shifts, changes, and goals.
- Ensuring the plan complies with any new laws or regulatory requirements.
- Addressing other organizational-specific maintenance goals.

During maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any team member is no longer with the company, the Disaster Recovery Lead will appoint a new team member.

Testing:

ConnectX is committed to ensuring the functionality of the DRP and will conduct testing every year. The plan will be tested using the following methods:

- Walkthroughs: Team members will verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks, or weaknesses. This method provides an opportunity to review the plan with a larger subset of people, drawing upon a correspondingly increased pool of knowledge and experiences.
- Simulations: Simulating a disaster without interrupting normal operations. This test will thoroughly assess hardware, software, personnel, communications, procedures, supplies, forms, documentation, transportation, utilities, and alternate site processing. Validated checklists will be used to provide a reasonable level of assurance.
- Parallel Testing: Conducted in conjunction with a checklist test or simulation, this involves processing historical transactions against backup files at the contingency processing site. Reports produced at the alternate site for the current business date should align with those produced at the primary processing site.
- Full-Interruption Testing: Activating the total DRP, this comprehensive test will be approached with caution due to potential costs and disruptions to normal operations. Due diligence from previous DRP phases is crucial before undertaking a full-interruption test.

Business Continuity Plans

Business Function Recovery Priorities

In the dynamic landscape of mobile services, ConnectX understands the critical importance of disaster recovery to maintain operational continuity. Should an unforeseen event disrupt its primary operational hub, ConnectX's disaster recovery teams will focus on recovering essential business functions, ensuring a swift return to normalcy. The recovery strategy centers around relocating operations to an alternate site while prioritizing the restoration of critical business functions.

2.1. Customer-Facing Services:

Customer Service and Support: Swiftly restore customer service and support functions to address inquiries, technical issues, and billing concerns. Provide uninterrupted assistance via phone and online channels.

Online Portal: Prioritize the recovery of online portal to ensure customers have seamless access to their accounts, billing information, and self-help resources.

2.2. Network Infrastructure:

Data Centres and High-Speed Network Backbone: Expedite the recovery of data centers, ensuring the availability of critical networking equipment, servers, and databases. Reinstate the high-speed, fibre-optic network backbone for reliable data transmission between locations.

2.3. IT Operations

IT Infrastructure: Prioritize the restoration of IT infrastructure, including servers, databases, and data centers, to secure the reliability and security of essential systems.

Software Updates: Rapidly apply software updates to protect against security vulnerabilities and enhance overall service efficiency.

2.4. Network Operations:

Network Monitoring: Swiftly reinstate the 24/7 Network Operations Centre (NOC) to monitor network performance, detect issues, and initiate a rapid response to minimize service disruptions.

Capacity Management and Vendor Relations: Optimize network resources for efficient usage, collaborating with equipment vendors and service providers to maintain and upgrade network components.

2.5. Financial Management:

Budgeting and Financial Planning: Prioritize the recovery of financial systems to manage budgets, track infrastructure investments, and monitor expenses.

Revenue Assurance and Financial Reporting: Implement measures to prevent revenue leakage, and promptly restore financial reporting systems to track revenue, expenses, and profitability.

2.6. Employee Operations:

Critical Staff Availability: Identify and ensure the availability of key personnel, including network engineers, customer service representatives, security personnel, and IT support specialists, to expedite the recovery process.

2.7. Business Working Methodology:

By aligning recovery priorities with these critical business functions, ConnectX aims to minimize downtime, maintain customer satisfaction, and swiftly restore its operations to full capacity after a disruptive event.

Hazard	Probability	Magnitude	Warning Duration	Risk Priority
Flooding	Highly Likely	Catastrophic	12+ hrs	High
Thunderstorms/Lightning/Hail	Likely	Critical	6 – 12 hrs	Medium
High Winds	Likely	Limited	3 – 6 hrs	Medium
Landslide	Possible	Limited	6 – 12 hrs	Medium
Earthquake	Possible	Limited	6 – 12 hrs	Medium

Hazard	Probability	Magnitude	Warning Duration	Risk Priority
Network Downtime	High	High	Low	High
Cybersecurity Breach	Medium	High	Medium	High
Software Failure	High	High	Low	High
Data Loss	Medium	High	Medium	High
Service Outage	High	High	Low	High
Power Outage	Medium	High	Medium	High
Equipment Failure	High	High	Low	High
Infrastructure Damage	Medium	High	Medium	High
Human Error	High	High	Low	High
Vendor Disruption	Medium	High	Medium	High
Regulatory Changes	Medium	High	Medium	High
Supply Chain Failure	High	High	Low	High
Communication Loss	Medium	High	Medium	High
Market Competition	High	High	Low	High
Employee Turnover	High	High	Low	High
IT System Overload	High	High	Low	High
Customer Complaints	Medium	High	Medium	High

8.2. Critical Business Functions

For the template Appendix.

8.2.1. Function: Customer Service Operations

Business Process to Complete:

Manage customer inquiries, subscriptions, and support through customer service representatives utilizing phone and online interactions. Utilize a local CRM system to track inquiries and subscriptions, along with standardized forms for issue resolution.

Supporting Activities:

Staff training on the local CRM system, escalation procedures for complex issues, periodic quality assurance checks on customer interactions in Urdu and English.

Lead Point of Contact (POC) and Alternate:

Customer Service Manager (Ali Khan) - [AliKhan@connectx.pk], Alternate (Sana Ahmed) - [SanaAhmed@connectx.pk].

Vendors and External Contacts:

CRM Software Provider (Local IT Solutions) - [info@localitsolutions.com.pk], Telephony Services Provider (PakTel) - [support@paktel.com.pk].

Vital Records:

Customer contact information, service records, subscription details in local databases.

Maximum Allowed Downtime:

Less than 24 hours.

Criticality:

High.

Required Resources:

25 employees, telephony systems, standardized customer forms in Urdu and English.

8.2.2. Function: Network Operations and Infrastructure Management

Business Process to Complete:

Manage and monitor the countrywide network infrastructure, troubleshoot technical issues, and ensure connectivity. Utilize local network diagnostic tools and hardware monitoring systems to identify and resolve network disruptions.

Supporting Activities:

Routine network maintenance by local technicians, periodic hardware checks, software updates compliant with local regulations.

Lead Point of Contact (POC) and Alternate:

Network Operations Manager (Hassan Ali) - [HassanAli@connectx.pk], Alternate (Fatima Khan) - [FatimaKhan@connectx.pk].

Vendors and External Contacts:

Network Hardware Vendor (Local Networks Ltd) - [sales@localnetworks.pk], Network Security Services (Secure Net) - [info@securenet.pk].

Vital Records:

Network configurations, hardware schematics, maintenance logs.

Maximum Allowed Downtime:

1 to 2 weeks.

Criticality:

High.

Required Resources:

15 employees, local network diagnostic tools, backup hardware systems.

This representation demonstrates how contact details might be displayed in a fictitious context, mirroring a real-world scenario without providing actual contact information.

8.2.3. Function: Financial Operations and Accounting

Business Process to Complete:

Manage financial transactions, invoicing, and payroll. Utilize accounting software compliant with local tax regulations and maintain accurate financial records.

Supporting Activities:

Regular auditing, compliance checks with tax laws, financial forecasting, and budgeting.

Lead Point of Contact (POC) and Alternate:

Finance Manager (Amir Khan) - [AmirKhan@connectx.pk], Alternate (Zara Ahmed) - [ZaraAhmed@connectx.pk].

Vendors and External Contacts:

Accounting Software Provider (Local Accounts Pro) - [support@localaccountspro.pk], Tax Consultant (TaxWise Consultants) - [info@taxwiseconsultants.pk].

Vital Records:

Financial statements, tax filings, payroll records, vendor invoices.

Maximum Allowed Downtime:

Less than 24 hours.

Criticality:

High.

Required Resources:

10 employees, accounting software, secure financial database.

8.2.4. Function: Human Resources Management

Business Process to Complete:

Manage employee records, recruitment, training, and compliance with Labor laws. Utilize HR management software to track employee data and manage benefits.

Supporting Activities:

Staff training programs, performance evaluation, legal compliance checks, and employee welfare programs.

Lead Point of Contact (POC) and Alternate:

HR Manager (Sadia Malik) - [SadiaMalik@connectx.pk], Alternate (Ahmed Khan) - [AhmedKhan@connectx.pk].

Vendors and External Contacts:

HR Software Provider (HR Pro Solutions) - [info@hrprosolutions.pk], Legal Advisor (Law wise Legal Consultants) - [advice@lawwise.pk].

Vital Records:

Employee contracts, training records, payroll information.

Maximum Allowed Downtime:

1 to 2 weeks.

Criticality:

Medium.

Required Resources:

8 employees, HR management software, compliance documents.

8.2.5. Function: Supply Chain Management

Business Process to Complete:

Manage procurement, inventory, and distribution channels. Utilize supply chain management software to track inventory levels and streamline logistics.

Supporting Activities:

Supplier relationship management, inventory forecasting, quality control checks.

Lead Point of Contact (POC) and Alternate:

Supply Chain Manager (Nadia Rehman) - [NadiaRehman@connectx.pk], Alternate (Ali Abbas) - [AliAbbas@connectx.pk].

Vendors and External Contacts:

Supply Chain Software Provider (Supplies Solutions) - [support@supplytechsolutions.pk], Logistics Partner (Logicise Logistics) - [info@logiwise.pk].

Vital Records:

Supplier contracts, inventory reports, logistics plans.

Maximum Allowed Downtime:

1 day to 1 week.

Criticality:

High.

Required Resources:

12 employees, supply chain software, inventory management tools.

8.3. Plan Activation Procedures

The designated Business Owner or assigned representative will commence the implementation of ConnectX's Business Continuity Plan.

Plan Activation During Normal Business Hours

In the event of a determination that ConnectX's facility in Islamabad is unsuitable for inhabitation due to unforeseen circumstances, the Business Owner or designated authority will promptly communicate the necessary steps to all personnel. Employees may receive instructions to either return home, await further guidance, or activate the Business Continuity Plan by relocating to the alternate site. Detailed directives regarding reporting for work or subsequent actions will be disseminated using the communication procedures outlined in Sections 4 and 6 of ConnectX's Business Continuity Plan.

Plan Activation Outside Normal Business Hours

If an unforeseen event occurs outside regular business hours, rendering the primary facility in Islamabad uninhabitable, the Business Owner or designated representative will initiate the Business Continuity Plan. This activation will follow the communication procedures detailed in Section 4 of ConnectX's Business Continuity Plan.

Actions upon Activation

Upon activating the Business Continuity Plan, the Business Owner or designated representative will take responsibility for promptly informing the alternate site, if applicable, of their impending arrival and the commencement of operational activities.

8.4. Internal Communication Procedures

Staff Accountability

Upon the evacuation of employees, customers, and guests, all personnel should gather at the primary assembly point and await further instructions.

Once assembled at the designated point, the following accountability measures must be taken:

Conduct headcount: Take attendance and note any missing and/or injured employees, customers, or guests.

Report missing and/or injured individuals: Notify the Business Owner or designated authority about any missing or injured personnel.

This information should be shared promptly with emergency first responders present at the scene.

The Business Owner or designated authority will decide on the most effective methods for communicating with staff, referencing the details provided in Section 6, Employee Contact List.

Employee Communication Methods:

Name	Work Email	Personal Email	Mobile Number
Ali Khan	AliKhan@connectx.pk	AliKhan@gmail.com	+92 300 123 4567
Sana Ahmed	SanaAhmed@connectx.pk	SanaAhmed@yahoo.com	+92 345 987 6543
Zara Malik	ZaraMalik@connectx.pk	ZaraMalik@hotmail.com	+92 333 555 8899
Amir Shah	AmirShah@connectx.pk	AmirShah@gmail.com	+92 300 111 2222
Fatima Ali	FatimaAli@connectx.pk	FatimaAli@yahoo.com	+92 321 222 3333
Usman Akhtar	UsmanAkhtar@connectx.pk	UsmanAkhtar@hotmail.com	+92 300 444 5555
Ayesha Raza	AyeshaRaza@connectx.pk	AyeshaRaza@gmail.com	+92 333 444 5555
Kareem Khan	KareemKhan@connectx.pk	KareemKhan@yahoo.com	+92 300 777 8888
Sarah Ahmed	SarahAhmed@connectx.pk	SarahAhmed@hotmail.com	+92 300 888 9999
Bilal Rizvi	BilalRizvi@connectx.pk	BilalRizvi@gmail.com	+92 333 555 6666
Amina Hasan	AminaHasan@connectx.pk	AminaHasan@yahoo.com	+92 300 333 4444
Yasir Farooq	YasirFarooq@connectx.pk	YasirFarooq@hotmail.com	+92 300 555 6666
Natasha Khan	NatashaKhan@connectx.pk	NatashaKhan@gmail.com	+92 300 111 2222
Arif Ali	ArifAli@connectx.pk	ArifAli@yahoo.com	+92 345 333 4444
Anam Fatima	AnamFatima@connectx.pk	AnamFatima@hotmail.com	+92 321 111 2222
Umair Aslam	UmairAslam@connectx.pk	UmairAslam@gmail.com	+92 333 777 8888
Mahnoor Khan	MahnoorKhan@connectx.pk	MahnoorKhan@yahoo.com	+92 333 888 9999
Adnan Ahmed	AdnanAhmed@connectx.pk	AdnanAhmed@hotmail.com	+92 321 999 0000
Sadia Hussain	SadiaHussain@connectx.pk	SadiaHussain@gmail.com	+92 300 456 7890

Salman Iqbal	SalmanIqbal@connectx.pk	SalmanIqbal@yahoo.com	+92 345 987 6543

8.5. Alternate Facilities and Telework Options

Alternate Facility Selection

When choosing an alternate facility, ConnectX prioritizes sites ensuring they can accommodate critical business functions in case the primary facility becomes unusable.

Considerations for Alternate Facilities

ConnectX considers several factors when selecting alternate facilities:

Distance from Primary Facility:

Driving distance: Approximately 15 miles.

Facility POC:

Name: Ahmed Khan

Title: Facilities Manager

Contact: +92 300 555 1234

Required Equipment:

IT server racks, backup network hardware, office supplies, essential documents.

Parking/Public Transit Accessibility:

Parking available for 50 vehicles. Accessible via the Blue Metro Line and Bus Route 22. Partial compliance includes wheelchair ramps and accessible restrooms.

Alternate Site Ranking Table

#	Site Address	Distance from Primary Facility	Facility POC	Required Equipment	Parking / Public Transit Accessibility
1	123 XYZ Avenue	15 miles	Ahmed Khan	IT equipment, office supplies	Parking available, Metro Line access
2	456 ABC Street	12 miles	Sarah Rahman	Backup network hardware, documents	Limited parking, Bus Route 22 access
3	789 PQR Road	18 miles	Ayesha Zafar	Office supplies, backup systems	Parking available, Metro Line access

8.6. Order of succession and Ddelegations of authority

Overview

Orders of succession within ConnectX are designed to offer clarity in leadership roles should key individuals become unavailable. Delegations of authority empower successors to legally act on behalf of critical positions in the organization for specific duties.

Orders of Succession

Orders of succession represent a formal, hierarchical listing of senior leadership roles, delineated by position, ensuring clear identification of authorized individuals who can step into these roles should the incumbent be unavailable due to absence, incapacity, or other reasons. These are crucial to maintaining operational efficiency during any disruptive incidents.

Delegations of Authority

Delegations of authority grant legal permission for designated successors in key senior leadership positions to make policy determinations and decisions, as necessary. These delegations specify the type and limitations of authority being transferred, such as signatory or purchasing authorization. Incumbents' duties are delegated to successors under various circumstances like absence, illness, leave, or termination, and are rescinded upon the incumbent's return.

Position to be Succeeded	**Successors**	**Delegated Authorities**	**Activation and Termination Triggers**
Senior Manager Finance	Asad Khan	Financial reporting, budget allocation	Activate: Incapacitated, Unavailable
Assistant Manager HR	Sara Ahmed	Recruitment, employee onboarding	Activate: Absence, Leave
Marketing Lead	Zahra Khan	Marketing strategies, campaign planning	Activate: Absence, Unavailability
Product Manager	Usman Ali	Product development, market research	Terminate: Return of Marketing Lead
IT Manager	Amir Khan	Network management, system administration	Activate: Incapacitated, Unavailable
Physical Security Lead	Fatima Malik	Access control, surveillance systems management	Activate: Leave, Unavailability
Security Lead	Raza Khan	Facility patrolling, incident response,	Activate: Leave, Unavailability

8.7. Plan Deactivation

Plan deactivation is the process of demobilizing the alternate facility and restoring critical business functions to the primary facility or a new facility that will permanently replace the damaged facility. Plan deactivation may not consist of an exact replacement of lost facilities, equipment, or processes. The goal of plan deactivation is to reestablish full capability in the most efficient manner. In some continuity incidents, extensive coordination may be necessary to backfill staff, procure a new operating facility, and re-establish IT infrastructure and vital records. When it is determined the COOP activation has ended, all personnel should be informed that the necessity for continuity operations no longer exists and the return to normal operations will begin.

Function	Supplies	Required Resources
Network Operations and Infrastructure	Network diagnostic tools, hardware monitoring systems	Trained local technicians, Backup hardware systems
Financial Operations and Accounting	Accounting software, financial records	Trained finance team, Secure financial database
Human Resources Management	HR management software, compliance documents	Trained HR team, Employee contracts
Supply Chain Management	Supply chain software, inventory management tools	Trained supply chain team
Legal and Compliance Management	Legal documents, compliance software	Legal team, Compliance specialists

8.8.Employee Contact Information

Employee Name	Title / Responsibility	Home / Cell Number	Personal Email Address
Ali Khan	Network Engineer	+92 300 123 4567	ali.khan@email.com
Sana Ahmed	Sales Manager	+92 345 987 6543	sana.ahmed@email.com
Zara Malik	HR Coordinator	+92 333 555 8899	zara.malik@email.com
Amir Khan	IT Support Specialist	+92 321 555 8888	amir.khan@email.com
Fatima Ali	Marketing Executive	+92 300 777 9999	fatima.ali@email.com
Ahmed Hassan	Customer Service Rep	+92 333 888 2222	ahmed.hassan@email.com
Maria Iqbal	Finance Analyst	+92 345 222 7777	maria.iqbal@email.com
Bilal Mahmood	Operations Manager	+92 321 333 4444	bilal.mahmood@email.com
Ayesha Shah	HR Manager	+92 300 111 8888	ayesha.shah@email.com
Usman Khan	Sales Representative	+92 333 444 0000	usman.khan@email.com
Hina Aziz	Project Coordinator	+92 345 666 3333	hina.aziz@email.com
Saad Malik	Legal Advisor	+92 321 777 4444	saad.malik@email.com
Sania Ilyas	Customer Support	+92 300 555 1111	sania.ilyas@email.com
Yasir Abbas	Procurement Specialist	+92 333 999 8888	yasir.abbas@email.com
Amina Riaz	Quality Assurance	+92 345 111 0000	amina.riaz@email.com
Farhan Mahmood	Business Analyst	+92 300 444 7777	farhan.mahmood@email.com
Fariha Khan	IT Security Specialist	+92 321 888 5555	fariha.khan@email.com
Imran Siddique	Operations Coordinator	+92 333 222 9999	imran.siddique@email.com

Rida Ali	Public Relations	+92 300 888 3333	rida.ali@email.com
Asad Iqbal	Software Engineer	+92 345 555 7777	asad.iqbal@email.com

8.9. Vendors Information

Vendor	Resource/Service	Contact Information
Local IT Solutions	IT Support Services	support@localitsolutions.pk
Reliable Power Inc.	Backup Power Systems	info@reliablepower.com.pk
SecureTech Security	Physical Security	security@securetech.pk
Swift Telecom	Telecommunications	sales@swifttelecom.pk
Green Office Supply	Office Supplies	orders@greenoffice.pk

Case 01:

Introduction: ConnectX Telecommunications, a leading provider of mobile services in the dynamic landscape of telecommunications, faces the ever-present challenge of maintaining operational continuity in the face of unforeseen events. In this case study, we explore how ConnectX leverages a robust Business Continuity Plan (BCP) to navigate through a scenario and ensure the swift recovery of critical business functions.

Scenario: A catastrophic flooding event has occurred in Islamabad, where ConnectX's primary operational hub is located. The flood has rendered the facility unsuitable for inhabitation, posing a significant threat to the company's operations. ConnectX must now activate its Business Continuity Plan to ensure the seamless recovery of essential business functions.

Business Continuity Plan Activation:

Communication of Activation:

Normal Business Hours: The Business Owner, Ali Khan, or the designated authority will promptly communicate the necessary steps to all personnel during regular business hours. Employees will receive instructions to either return home, await further guidance, or activate the Business Continuity Plan by relocating to the alternate site.

Outside Normal Business Hours: If the event occurs outside regular business hours, the Business Owner or designated representative will initiate the plan, following communication procedures outlined in the BCP.

Actions upon Activation:

Upon activating the BCP, Ali Khan will inform the alternate site (selected from the prioritized list) of their impending arrival and the commencement of operational activities.

Recovery Priorities: ConnectX follows a structured approach to recover critical business functions. Here are some key priorities in the recovery process:

Customer-Facing Services:

Customer Service and Support: Swift restoration of customer service functions to address inquiries via phone and online channels.

Online Portal: Priority on the recovery of the online portal to ensure seamless customer access to accounts and self-help resources.

Network Infrastructure:

Data Centers and Network Backbone: Expedited recovery of data centers and the high-speed network backbone for reliable data transmission.

IT Operations:

IT Infrastructure: Restoration of servers, databases, and data centers to ensure the reliability and security of essential systems.

Software Updates: Rapid application of software updates to enhance service efficiency and security.

Network Operations:

Network Monitoring: Swift reinstatement of the 24/7 Network Operations Centre (NOC) for proactive monitoring and issue resolution.

Capacity Management: Optimization of network resources in collaboration with vendors and service providers.

Financial Management:

Budgeting and Financial Planning: Priority on the recovery of financial systems for effective budget management.

Revenue Assurance: Implementation of measures to prevent revenue leakage.

Employee Operations:

Critical Staff Availability: Identification and availability assurance of key personnel for an expedited recovery process.

Risk Assessment: ConnectX has conducted a comprehensive risk assessment, identifying potential hazards such as flooding, thunderstorms, and earthquakes. Each hazard is categorized based on probability, magnitude, warning duration, and risk priority.

Critical Business Functions: ConnectX has defined critical business functions, including Customer Service Operations, Network Operations and Infrastructure Management, Financial Operations and Accounting, Human Resources Management, and Supply Chain Management.

Orders of Succession and Delegations of Authority: The company has established clear orders of succession and delegations of authority, ensuring leadership roles are filled promptly in case key individuals are unavailable.

Employee and Vendor Information: ConnectX maintains up-to-date contact information for employees and vendors, crucial for communication during and after the activation of the BCP.

Plan Deactivation: Once the operational capability is reestablished, ConnectX will commence the plan deactivation process, restoring critical business functions to the primary facility or a new facility, efficiently coordinating staff, and re-establishing IT infrastructure.

Lessons Learned: Post-incident, ConnectX will conduct a thorough review of the activation and recovery process, identifying lessons learned and areas for improvement to enhance future response capabilities.

Case 02:

ConnectX Technologies, a leading mobile services provider, faced a critical risk when a medium-probability, high-magnitude power outage disrupted operations at its primary facility in Islamabad. In response, ConnectX swiftly activated its Business Continuity Plan (BCP), deploying a robust technical strategy to navigate the challenges posed by the outage.

Business Continuity Plan Activation:

Communication of Activation:

Normal Business Hours:

During regular business hours, the designated Business Owner or representative assumed responsibility for communicating activation steps to all personnel. This involved disseminating detailed instructions regarding relocation to the alternate site or guidelines for remote work.

Outside Normal Business Hours:

Outside regular business hours, the Business Owner or representative took charge, initiating the BCP by following outlined communication procedures. This proactive approach ensured a seamless transition even during non-standard working hours.

Actions upon Activation:

Upon BCP activation, ConnectX prioritized communication with the alternate site. Employees received instructions tailored to the severity of the situation, including guidance on relocation, or facilitating remote work arrangements. This step was critical in maintaining operational continuity in the face of the outage.

Customer Service Operations:

Business Process:

ConnectX focused on the swift and efficient management of customer inquiries, subscriptions, and support. The emphasis was on utilizing phone and online interactions to sustain seamless customer service.

Supporting Activities:

To bolster customer service operations, ConnectX invested in staff training on the local Customer Relationship Management (CRM) system. Additionally, periodic quality assurance checks were implemented to ensure the highest standards in customer interactions.

Lead Point of Contact (POC):

The Customer Service Manager, Ali Khan, served as the central point of contact, ensuring a streamlined and coordinated approach to customer-facing activities.

Network Operations and Infrastructure Management:

Business Process:

ConnectX prioritized the management and monitoring of its countrywide network infrastructure. This encompassed troubleshooting technical issues and ensuring continuous connectivity to minimize the impact of the power outage.

Supporting Activities:

To fortify network operations, routine maintenance by local technicians was conducted. Periodic hardware checks and compliant software updates were implemented to maintain the integrity and efficiency of the network.

Lead Point of Contact (POC):

Hassan Ali, the Network Operations Manager, assumed a leadership role, overseeing the technical aspects of network infrastructure management.

Financial Operations and Accounting:

Business Process:

In financial operations and accounting, ConnectX focused on the seamless management of transactions, invoicing, and payroll. The use of accounting software compliant with local tax regulations was central to this process.

Supporting Activities:

ConnectX implemented regular auditing and compliance checks, ensuring adherence to financial regulations. Financial forecasting and budgeting activities were undertaken to maintain financial stability.

Lead Point of Contact (POC):

Amir Khan, the Finance Manager, played a pivotal role in overseeing financial operations, providing stability during the outage.

Alternate Facilities and Telework Options:

ConnectX's BCP included a well-defined strategy for relocation to an alternate site based on predefined criteria. Proximity, accessibility, and equipped facilities were meticulously considered to facilitate a smooth transition in the event of facility displacement.

Order of Succession and Delegations of Authority:

The BCP outlined clear orders of succession for key leadership roles, ensuring that designated successors could seamlessly assume responsibilities in the absence of key individuals. Delegations of authority were designed to facilitate a smooth transition, specifying the type and limitations of authority being transferred.

Plan Deactivation:

The plan deactivation process involved the demobilization of the alternate facility and the restoration of critical business functions to the primary or a new facility. The overarching goal was to reestablish full capability efficiently, recognizing that continuity operations were no longer necessary.

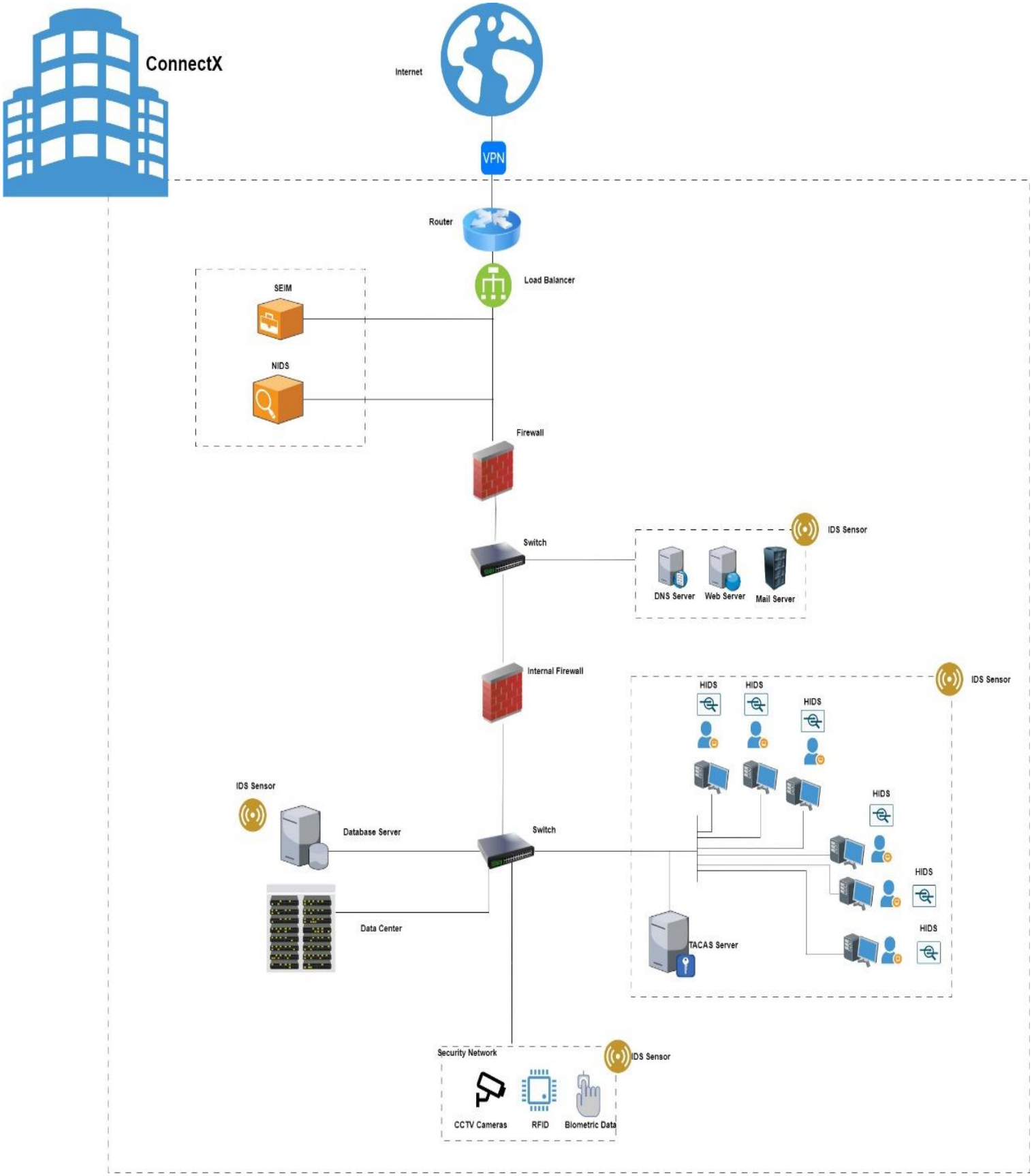
NOVEMBER 29, 2023

Security Architecture

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797


ConnectX
Internet
VPN
Router
Load Balancer
SEIM
NIDS
Firewall
Switch
IDS Sensor
DNS Server
Web Server
Mail Server
Internal Firewall
IDS Sensor
HIDS
HIDS
HIDS
HIDS
HIDS
HIDS
TACAS Server
IDS Sensor
Database Server
Switch
Data Center
Security Network
IDS Sensor
CCTV Cameras
RFID
Biometric Data

NOVEMBER 29, 2023

Physical Security Plan

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797

ConnectX, a leading mobile service provider, has successfully implemented a robust Physical Security Plan to safeguard its headquarters in downtown Islamabad. This comprehensive plan ensures the safety of personnel and the security of its infrastructure.

Contact List:

Name	Title	Phone Number	Email
Asad Ali	Security Head	+92 300 123 4567	asad.ali@example.com
Farhan Khan	Security Supervisor	+92 345 987 6543	farhan.khan@example.com
Saba Malik	Security Officer	+92 333 555 8899	saba.malik@example.com
Usman Ahmed	Security Officer	+92 300 111 2222	usman.ahmed@example.com
Ahmed Salah	Security Officer	+92 345 333 4444	ayesha.abbas@example.com
Bilal Shah	Security Officer	+92 333 666 7777	bilal.shah@example.com

1. **Building Security:**

Access Control: Biometric authentication and card access systems are actively regulating entry to sensitive areas, continuously updated to reflect role-based permissions.

Security Personnel: Trained security personnel equipped with conflict resolution skills and emergency response training ensure a secure environment.

Intrusion Detection Systems: State-of-the-art systems installed on windows and doors are regularly tested to maintain efficiency.

2. **Wall Security:**

A secure perimeter with anti-climbing features is maintained to deter unauthorized access. Regular inspections and motion-activated lighting contribute to heightened security.

3. **Surveillance Cameras:**

- Strategically placed cameras cover entry/exit points and blind spots, monitored 24/7 in a dedicated security operations center.

4. **Generators:**

- Securely placed and accessible only to authorized personnel, the generators undergo regular maintenance and testing to ensure operational readiness.

5. **IT Labs:**

Stringent access controls, including biometric authentication, ensure limited access. Continuous monitoring through security cameras maintains vigilance.

6. **CCTV Coverage on Each Floor:**

Comprehensive CCTV coverage on every floor ensures monitoring of all common areas for enhanced security.

7. **Employee Parking Areas:**

Well-lit parking areas with surveillance cameras and strict access controls guarantee employee safety.

8. **Employee Workspaces:**

Card access systems and panic buttons ensure secure work environments, allowing prompt response during emergencies.

9. **Gate Entrance Policies and Security for Floor Gates:**

Stringent gate entrance policies for visitors are in place, along with access controls on floor gates.

10. **Emergency Response Plan:**

An extensive emergency response plan covers evacuation procedures, communication systems, and collaborations with local law enforcement.

11. **Regular Audits and Training:**

Regular security audits, corrective actions based on findings, and ongoing employee security awareness training are part of the routine.

12. **Collaboration with Local Law Enforcement:**

Collaborations with local law enforcement agencies ensure swift response and additional security support.

13. **Fire Safety Measures:**

Fire safety equipment, evacuation routes, and regular drills ensure preparedness for fire emergencies.

14. **Data Security:**

Enhanced data security measures, including restricted access, encryption, and regular backup testing, maintain data integrity.

15. **Visitor Management System:**

A robust visitor management system effectively monitors and tracks all visitor activities.

16. **Cybersecurity Protocols:**

Integrated robust cybersecurity protocols to protect against cyber threats are continuously updated and tested.

17. **Public Areas Security:**

Implemented access controls and surveillance in public areas prevent unauthorized access.

18. **Biometric Access for Data Centers:**

Biometric access adds an extra layer of security to critical areas such as data centers and ACL (access control list).

ConnectX's commitment to maintaining and improving these implemented security measures reflects its dedication to ensuring the safety and security of its infrastructure and personnel in G9, Islamabad. Regular reviews and collaborations ensure the continued effectiveness of these measures.

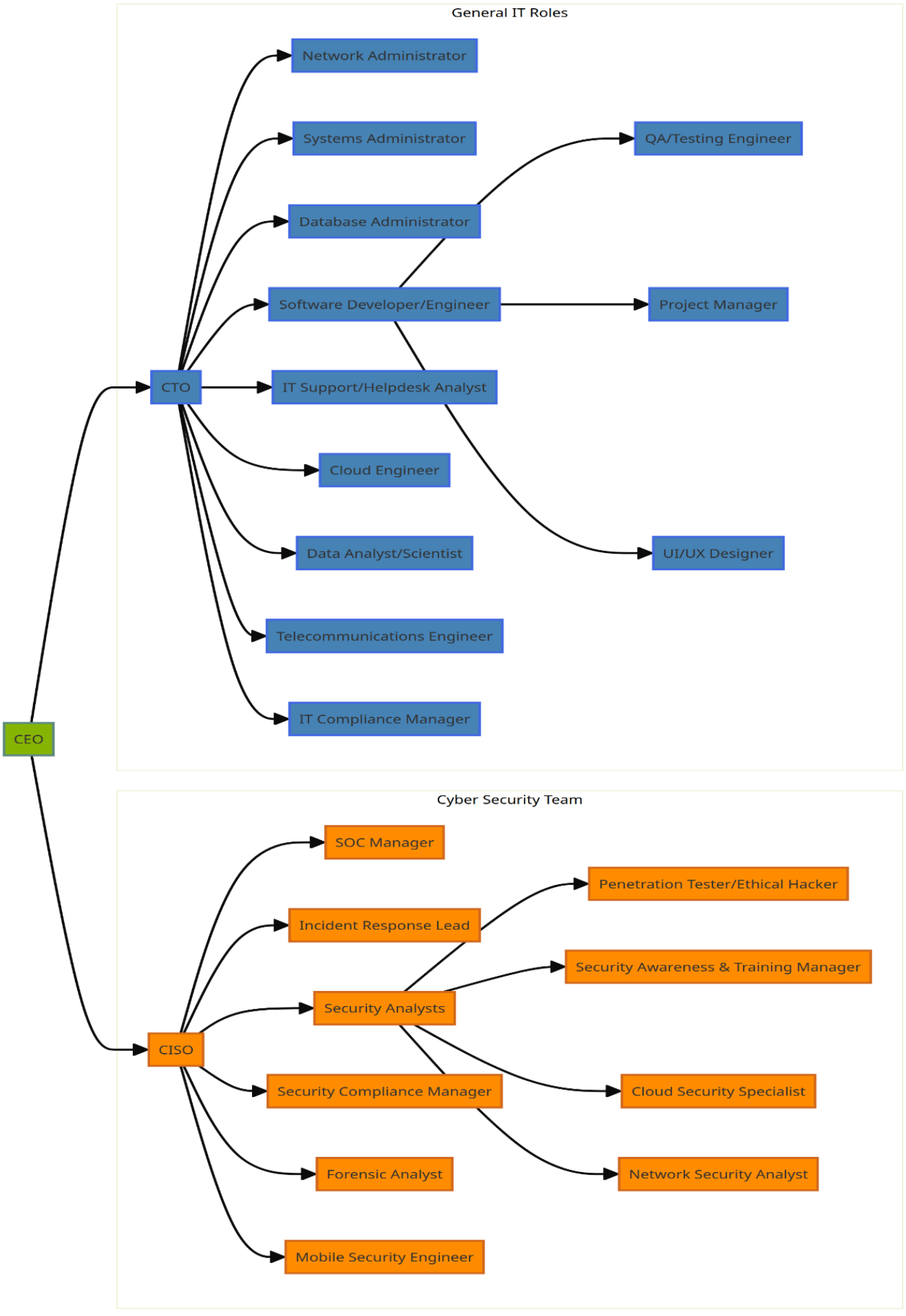
NOVEMBER 29, 2023

IT/Security Team Hierarchy

CONNECTX

INFORMATION SECURITY MANAGEMENT PLAN

MUSAAB IMRAN 20I-1794
MUHAMMAD USMAN SHAHID 20I-1797


General IT Roles
Network Administrator
Systems Administrator
QA/Testing Engineer
Database Administrator
Software Developer/Engineer
Project Manager
CTO
IT Support/Helpdesk Analyst
Cloud Engineer
Data Analyst/Scientist
UI/UX Designer
Telecommunications Engineer
IT Compliance Manager
CEO
Cyber Security Team
SOC Manager
Penetration Tester/Ethical Hacker
Incident Response Lead
Security Awareness & Training Manager
Security Analysts
CISO
Security Compliance Manager
Cloud Security Specialist
Forensic Analyst
Network Security Analyst
Mobile Security Engineer