Information Technology, Data Protection and Cyber Security Manual

Edition No. I

Caritas
JERUSALEM

Approval Statement

This manual has undergone comprehensive review by the Caritas Jerusalem Executive Committee on February 13, 2024, and has been officially approved by the President of Caritas Jerusalem his Beatitude Cardinal Pierbattista Pizzaballa on February 19, 2024.

The effective date of this manual is the 1st of April 2024.

CARITAS JERUSALEM

President's Signature:

Caritas JERUSALEM

Table of Contents

Chapter 1: Introduction

1. Purpose of Information Technology Policies and Procedures

The purpose of the Information Technology and Cybersecurity Manual is to establish clear policies and procedures for the secure and effective use of information technology resources within Caritas Jerusalem. This manual outlines the principles, policies, and procedures that internal and external personnel must follow to safeguard our IT Resources, maintain the confidentiality and integrity of information, and ensure the effectiveness of our IT systems. By following these guidelines, Caritas aims to create a secure IT environment, protect against cyber threats, and ensure responsible and appropriate use of technology across the organization.

Information Technology is an important and critical component of daily business. This Policy seeks to ensure that all IT resources, including hardware, software, network equipment, efficiently:

- serve the primary business functions.
- provide security for employees' electronic data.
- protect the integrity of private and confidential information and business data.
- comply with internal regulations.

Caritas Jerusalem must restrict access to confidential and sensitive data to protect it from being lost or leak.

Importance of Following Guidelines for IT Security:

1. Protection Against Cyber Threats: Guidelines provide a defense against various cyber threats, including unauthorized access, malware, and data breaches, protecting Caritas from potential harm.
2. Confidentiality and Data Integrity: Adhering to security guidelines ensures the confidentiality of information and the integrity of data, preventing unauthorized access and maintaining the accuracy of critical data.
3. Operational Continuity: By following security practices, Caritas ensures the availability and continuity of IT services, minimizing disruptions and maintaining operational efficiency.
4. Compliance and Legal Requirements: Adherence to security guidelines ensures compliance with industry regulations and legal requirements, preventing legal consequences and safeguarding the organization's reputation.
5. Financial and Reputational Protection: Following guidelines helps prevent financial losses associated with security breaches and protects the organization's reputation, fostering trust among stakeholders.
6. Employee and partners Trust: Security measures instill confidence in employees and partners, assuring them that their sensitive information is handled responsibly and securely.
7. Prevention of Productivity Loss: Security incidents can lead to downtime and productivity loss. Adhering to guidelines minimizes disruptions, allowing smooth business operations.

In summary, the IT Security Manual plays a crucial role in establishing a secure digital environment. Following its guidelines is essential for safeguarding assets, maintaining compliance, and protecting the organization's overall well-being, including its financial stability and reputation.

Chapter 1: Introduction

1.2 Applicability

The IT and Cyber Security manual serves as guidance to Caritas Jerusalem and its partners and is applicable to all operations activities, processes, and procedures.

The guidelines in this manual are minimum requirements and are applicable to all activities. If a donor stipulates strict IT rules and procedures, those rules and procedures shall prevail. If a donor stipulates less strict IT rules and procedures, this manual shall be applicable to the process.

1.3 Directory terms

This manual is a document that can be implemented and developed after the approval of the Board of Directors and Executive Committee. This manual target all those who are involved in the operations of Caritas Jerusalem in particular, in addition to the concerned employees and administrators.

1.4 Manual Updates

The IT manual is dynamic and can be updated annually based on operations requirements, user experience and best practices to ensure its relevance. Suggested alteration or modification of the policies must be approved in writing by the Executive Committee. Furthermore, the organization may change, delete, suspend or discontinue any part or parts of the policies in this Manual at any time provided that proper employees' notifications are done on a timely manner.

1.5 Terminology and Abbreviations

The terms listed below have the following definitions:

CJ	Caritas Jerusalem
The Organization	Caritas Jerusalem
Board of Directors (BoD)	Caritas Jerusalem Board of Directors
Executive Committee (ExCom)	Caritas Jerusalem Executive Committee
Chairperson	President of Board of Directors
Secretary General / CEO / Executive Director	Caritas Jerusalem Secretary General
Head of Finance / Finance Manager (HoF)	Caritas Jerusalem Financial Manager
IT Manual	The Information Technology and Cyber Security Policies and Procedures
Senior Management Team (SMT)	Heads of Departments

Chapter 1: Introduction

Receipt and Acknowledgment of the Manual

(To be placed in the employee personal file)

All Staff with no exception noted shall read the following statements, sign below, and return to the Human Resources Officer.

Understanding and Acknowledging Receipt of the Organization IT Manual
I have received and read a copy of the Organization IT Manual. I understand that the policies and procedures described within are applicable to all IT transactions with no exceptions noted. I understand that adherence to those policies and procedures will be utilized. In part, to assess my work performance evaluation. I also understand that the manual is subject to change at the sole discretion of Caritas Jerusalem at any time provided that a notice of change will be timely communicated to me.

Confidential Information
I am aware that during the course of my employment confidential information will be made available to me. I understand that this information is proprietary critical to the successful implementation of Caritas Jerusalem objectives and therefore must not be given out or used outside the Organization premises. In the event of termination of employment, whether voluntary or involuntary, I hereby agree not to utilize, exploit or discuss this information with any other individuals or entities.

Employee Name	Position
Employee Signature	Date

Chapter 1: Introduction

CONFIDENTIALITY PLEDGE FOR ALL CARITAS STAFF

I understand that I require information to perform my duties at Caritas Jerusalem CJ. This information may include but is not limited to, information on Patriarchs, Bishops, Priests, religious community, board members, executive committee members, employees, students, families, other workforce members, donors, beneficiaries, research, and financial and business operations and strategies. Some of this information is made confidential by law or by Caritas Jerusalem CJ policies. Confidential information may be in any form, e.g., written, electronic, oral, overheard or observed. Access to all confidential information is granted on a need-to-know basis. A need-to- know is defined as information access that is required in order to perform my work duties

I pledge to review the Caritas Jerusalem CJ policies on confidentiality and privacy. I will access, use and disclose confidential information in keeping with these policies and only on a need-to-know basis. Before I make any other use or disclosure of confidential information, I will contact my supervisor, manager or Secretary General (if applicable) in order to obtain proper permission.

I will not disclose confidential information to other initiations, official offices, organizations, relatives, co-workers or anyone else except as permitted by Caritas Jerusalem CJ policies and applicable law and as required to perform my work.

I will protect the confidentiality of all confidential information, at Caritas Jerusalem CJ and after I leave. All confidential information remains the property of Caritas Jerusalem CJ and may not be removed or kept by me when I leave Caritas Jerusalem CJ except as permitted by Caritas Jerusalem CJ policies or specific agreements or arrangements applicable to my situation.

It is important that the entire Caritas Jerusalem CJ share a culture of respect for confidential information. To that end, if I observe access to or sharing of confidential information that is or appears to be unauthorized or inappropriate, I will try to make sure that this use or disclosure does not continue and report any abuse of information when applicable. This might include advising the person involved that they may want to check the appropriateness of the use or disclosure with Caritas Jerusalem CJ management.

I understand that signing this pledge and complying with its terms is a requirement for me to work, at Caritas Jerusalem CJ.

If I violate this pledge, I will be subject to disciplinary action. In addition, under applicable law, I may be subject to criminal or civil penalties.

I have read the above pledge and agree to be bound by it.

Employee Name	Position
Employee Signature	Date

Chapter 2: Acceptable Use Policy

Section 1: Guidelines for the acceptable use of organization's IT resources.

The Acceptable Use Policy (AUP) outlines the guidelines and rules for the required and ethical use of the organization's information technology resources. These guidelines are designed to ensure the security, integrity, and appropriate use of IT assets and to promote a safe and productive computing environment for all users.

This policy applies to all employees, service providers, and any other individuals granted access to the organization's IT resources.

Guidelines:

- Authorized Use: IT resources are to be used solely for related activities that align with the organization's mission and objectives.
- User Accounts: Users must only access IT resources for which they have authorized permissions. Sharing login credentials is strictly prohibited.
- Data Protection: Users are responsible for safeguarding information and preventing unauthorized access or disclosure. Encryption process and software's should be used for maintaining and transferring sensitive data.
- Internet and Email Usage: Internet and email services are to be used for business purposes. Users should avoid accessing inappropriate or malicious websites and exercise caution with email attachments and links. It is prohibited to use emails for personal purposes.
- Software: Only licensed and approved software should be installed and used. Users must refrain from attempting to install or use unauthorized and non-licensed software.

- Hardware and Equipment: IT hardware should be used for organization operations and maintained in good condition. Users must report any hardware malfunctions or damage promptly to the IT Specialist.

- Network Security: Users must not attempt to override network security and disable related applications, including unauthorized access to network resources. Wireless network connections should be secured with strong encryption and passwords. It is prohibited to connect personal devices to the Caritas Network.

- Social Media and Online Presence: Representing the organization on social media should adhere to established guidelines. Employees should be careful when expressing personal opinions online, especially when related to the organization.

- Prohibited Activities: Engaging in any form of cyberbullying, harassment, or the creation or distribution of offensive content is strictly prohibited.

- Unauthorized attempts to gain access to IT systems or data, or any form of hacking, is strictly prohibited.

- Reporting Violations: Users are obligated to report any suspected violations of this policy to the IT Specialist, HR Officer or appropriate authorities promptly.

- Consequences of Violations: Violations of this Acceptable Use Policy may result in disciplinary action, including but not limited to warnings, suspension of IT privileges, and termination of employment or contracts. Legal action may be taken in cases of serious misconduct.

Chapter 2: Acceptable Use Policy

Section 2: Prohibited Activities and Consequences for Policy Violations:

Prohibited Activities:

- Unauthorized Access: Unauthorized access or use any IT system, data, or network resources without proper authorization are strictly prohibited.

- Malicious Software: Intentional installation or distribution of malicious software, including viruses, worms, trojan horses, or other forms of malware, is strictly prohibited.

- Data Manipulation: Unauthorized alteration, deletion, or manipulation of data without proper authorization is strictly prohibited.

- Unauthorized Hardware/Software Modifications: Modifying or attempting to modify hardware or software configurations without proper authorization is strictly prohibited.

- Inappropriate Content: Creation, transferring, or storage of any content that is offensive, harassing, discriminatory, or in violation of applicable laws is strictly prohibited.

- Cyberbullying and Harassment: Engaging in cyberbullying, harassment, or any form of offensive behavior towards others using IT resources is strictly prohibited.

- Unauthorized Disclosure: Unauthorized disclosure of sensitive or confidential information to external parties or unauthorized individuals is strictly prohibited.

Consequences for Policy Violations:

- Verbal or Written Warning: Minor violations may result in a verbal or written warning, clearly communicating the nature of the violation and the expected corrective action.

- Termination of Employment or Contract: Violations of the organization's security policy, reputation, or legal standing may lead to termination of employment or contractual agreements.

- Legal Action: In cases of criminal activities or serious breaches, the organization reserves the right to pursue legal action against the individuals involved.

- Appeals Process: Individuals subject to consequences have the right to appeal. Appeals should be submitted in writing to the designated authority within a specified timeframe. The organization will review appeals in a fair manner.

- Policy Acknowledgment: All users are required to read, understand, and acknowledge this policy. Failure to comply with these guidelines may result in disciplinary action. Regular training and awareness programs will be conducted to ensure ongoing adherence to these policies.

Chapter 3: User Account Management:

Section 1: Procedures for creating, modifying, and deactivating user accounts and Emails.

A) Creating user accounts and emails.

1. Human Resource Officer submits a request for new account creation to the IT Specialist.
2. The IT Administrator reviews the request for completeness and accuracy.
3. The request is forwarded to the Secretary General for approval.
4. Upon approval, the IT Administrator creates the new account following established security guidelines.
5. Account credentials are securely communicated to the Account Owner and must be changed on the first login by account owner.

B) Modifying user accounts and emails.

1. In case of account modification or changes in user permission, account owner should submit a documented request.
2. The Human Resource Officer reviews the need for modification for the daily activities of account owner. If applicable, the HR Officer may coordinate the modification with the head of department.
3. The IT Administrator reviews the request for completeness and accuracy.
4. The request is forwarded to the Secretary General for approval.
5. Upon approval, the IT Administrator modifies the account following established security guidelines.
6. Account Owner notified for the modification.

C) Deactivating user accounts and emails.

1. Upon end of employment for account owner, human resource officer submits a request for deactivating account to the IT Specialist.
2. The IT Administrator reviews the request for completeness and accuracy.
3. The request is forwarded to the Secretary General for approval.
4. Upon approval, the IT Administrator follows the procedures to obtain backup and safely deactivate the account following established security guidelines.
5. The Secretary General may request to keep an email account active for terminated employee and auto-forward emails to another email account for specific period.

Chapter 3: User Account Management:

Section 2: Password Policies and Guidelines:

The default password is available from the IT administrator. Users must change the password as soon as they logon and must not share it out with anyone. Instructions for changing the password are available by pressing Ctrl-Alt-Delete simultaneously on any windows machine. If the user forgot the password, he/she must contact the IT specialist.

1. Password Complexity: Minimum Length: Set a minimum password length. Must be a combination of uppercase and lowercase letters, numbers, and special characters to enhance complexity.

2. Password Change Frequency: Mandate periodic password changes to reduce the risk of unauthorized access.

3. Password History: Prohibit the reuse of three previous passwords to enhance security.

4. Account Lockout: Failed Login Attempts: Implement an account lockout policy for 15 minutes after five consecutive failed login attempts to deter brute-force attacks. Lockout Duration: Define a lockout duration and communicate it to users.

5. Two-Factor Authentication (2FA): Encouragement: Encourage or require the use of two-factor authentication for an added layer of security.

6. Password Recovery: Implement secure password recovery mechanisms to help users regain access to their accounts without compromising security.

7. Communication:
a. Clearly communicate password policies to all users during onboarding and periodically through reminders.
b. Issue notification regarding potential threats and the importance of maintaining strong passwords.

8. Multi-Account Considerations:
Unique Passwords: Encourage users not to reuse passwords across multiple accounts to prevent login user accounts if one account is compromised.

9. Mobile Device Security:
Emphasize the importance of securing passwords on mobile devices through PINs, biometrics, or other secure methods.

10. Monitoring:
Implement monitoring systems to detect suspicious login activity and enforce password policies consistently.

Implementing and regularly reviewing these password policies and guidelines contributes to creating a robust defense against unauthorized access and security threats. Regular updates to policies and ongoing user education are essential components of an effective password security strategy.

Chapter 4: Data Security and Protection

Section 1: Security of Information

Caritas Jerusalem will follow the guidance of the IASC Operational Guidance on Data Responsibility in Humanitarian Action, 2023 in the responsibility for data protection. (Annex One)

Financial Information Access and Security

The information in this section applies to activities information, including the followings:
- Network locations of shared files and common areas of use, mainframe, local area networks, and personal computers;
- Accounting software and systems and applications used for electronic processing of the Organization;
- Users of those systems and applications; and
- Personnel, who install, develop, maintain, and administer those systems and applications.

Authorization for Use of Financial Information

Other Organizations – Organizations outside of Caritas's needs to use financial information maintained by the Caritas (electronic and paper copy) must submit a request to the Secretary General for approval.
Auditors – Due to the scope and nature of their work, external auditors have read-only access to relevant information from computer or printed files and records.

Responsibilities

Anyone accessing the Organization's activities information must preserve the security and confidentiality of it, because they assume a responsibility concerning the information. Such information is to be used only for conducting the Organization's activities, or as authorized.

The employees shall keep information confidential and to refrain from disclosing confidential information or transferring papers, documents or any form of information relating to the work of the Organization to any person, body, or other entity unless approved by the Secretary General, or external auditors under thier scope of work, or required by law in accordance with a judicial decision and shall not make any actions and statements affecting or causing material or moral damage to the Organization.

1. The employee is obliged to safeguard all the secrets of the Organization and is prohibited from disclosing matters which he/she has access to, by virtue of his/her job, and in case of violation, the penalties shall be applied in accordance with the applicable regulations.
2. An employee shall not keep to himself/herself the original copy of any document or retain a copy of any document to the Organization which should remain confidential in nature or under instructions, nor shall he/she disclose matters which he/she has access to which should remain confidential in nature or under instructions.
3. Employees are expected to exercise responsible, ethical behavior when using the Organization's computers, information, networks, or resources for activities information purposes. Individual responsibilities include preserving the confidentiality and security of data to which they have been granted access and ensuring that data are used for and in the conduct of Organization's activities. These responsibilities include the proper storage, access control, and disposal of private and confidential data presented to the user in any form. Individuals must also report known or suspected security violations to the Organization.

Chapter 4: Data Security and Protection

Data Custodian

The Organization's senior management has delegated operational data control to various departments known as data custodians. Department heads or delegates, as data custodians, are authorized to grant permission to access data maintained by them to their employees when necessary for the efficient management of the Organization. Their responsibilities include:

- Identifying and classifying data that are collected and maintained;
- Authorizing access to data;
- Interpreting pertinent laws and the Organization's policies which determine the levels of confidentiality and security required for data;
- Supporting users in accessing and interpreting data;
- Providing guidance to the information security officers in establishing appropriate levels of security and confidentiality; and
- Reviewing security violations for appropriate action.

Ownership

The Organization owns all information (data, programs, and procedures) gathered, stored, or maintained for activities purposes. This ownership includes all forms of information—electronic or printed. It includes all copies of information on mainframe, personal computers, and local area networks, wherever the equipment or networks are located.

Violation

Violation of any provision of this section may cause the Organization to:

- Limit the individual's access to the Organization's systems;
- Initiate legal action;
- Require the violator to provide restitution for any improper use of service; or
- Enforce disciplinary sanctions in accordance with the relevant Organization's policy.

Confidentiality Pledge Form

All staff must sign the confidentiality pledge form; the signed form should be kept in the employee’s file.

Chapter 4: Data Security and Protection

Section 2: Cyber Security Policy

Information Technology (IT) is an important and critical component of daily business at the Organization. This Policy seeks to ensure that all IT resources, including hardware, software, network equipment, efficiently:

- Serve the primary activities functions;
- Provide security for employees' electronic data;
- Protect the integrity of the private and confidential information and data; and
- Comply with our regulations, to deliver our services to our partners as safe and secure as possible.

The Organization must restrict access to confidential and sensitive data to protect it from being lost, leak, or compromised in order to avoid adversely impacting our beneficiaries, incurring penalties for non-compliance and suffering damage to our reputation. At the same time, we must ensure users can access data as required for them to work effectively.

The Organization shall provide all employees and contracted third parties with access to the information they need to carry out their responsibilities as effectively and efficiently as possible. All financial information, as well as data of beneficiaries, partners, and vendors must be securely taken care of. All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

Protection of Personal and Organization Devices
When employees use their devices to access their emails or accounts, they introduce security risks to our data. It is advisable to keep both their personal and the Organization-issued computer and cell phone secure. The employees should ensure the following:

- Keep all devices password protected;
- Install and update a complete antivirus software;
- Avoid leaving their devices exposed or unattended;
- Install security updates of browsers and systems on a timely basis;
- Log into the Organization accounts and systems through secure and private networks only;
- Avoid accessing internal systems and accounts from other people's devices or lending their own devices to others;
- Look after their work devices properly as if it's their own;
- Avoid inserting personal storage devices on their work computers such as USB flash drives, external hard drives, and hard disks. Unless necessary, scan all removable devices for viruses first; and
- Regularly run anti-virus and anti-malware scans to their devices.

Chapter 4: Data Security and Protection

Email Safety

Scams and malware usually spread through emails. All employees need to know about scams, breaches, and malware so they can better protect our infrastructure. Emails often host scams and malicious software, to avoid virus infection, data theft, malicious software, and email scams, the Organization instructs employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained;
- Be suspicious of clickbait titles;
- Check email and names of people they received a message from to ensure they are legitimate;
- Report a phishing email if they think it is not safe; share any suspicious emails to IT Specialist as an attachment to investigate and issue organizational level alerts of phishing emails.
- Share work email address to people you trust;
- Be aware of opening emails from contacts you do not know;
- Check if the sender's name is consistent with their email;
- Inspect the email's domain if it is the Organization/vendor's legitimate domain;
- Be suspicious of attachments and links from the emails you receive, especially if it's from contacts they do not know;
- Be on the lookout for inconsistencies, grammar mistakes, spammy messaging, and too good to be true promises;
- Enable anti-spam and anti-malware scanners to flag spam, scam, and junk emails.
- Personal use of of the organization's emails is strictly prohibited.

Manage Passwords Properly

This policy applies to all employees and anyone who has permanent or temporary access to the systems and hardware. Passwords help keep accounts secure, but if passwords seem easy to remember, they are probably easy to hack as well. Password leaks are dangerous since they can compromise our entire infrastructure. The Organization advises our employees to:

- Choose passwords with at least eight characters, including capital and lower-case letters, numbers, and symbols;
- Avoid information that can be easily guessed like birthdays, name, family name, ID number;
- Enable two-factor authentication to all your accounts;
- Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done;
- The passwords have expiration policy that will obligate periodic passwords change.
- Avoid having the same password for many emails and accounts;
- Use the same guidelines stated above when creating your new passwords.

Chapter 4: Data Security and Protection

Transfer Data Securely

Transferring data introduces security risk. Employees must:

- Avoid transferring sensitive data (beneficiary information, employee records) to other devices or accounts unless necessary;
- Share confidential data over the organization network or system and not over public Wi-Fi or private connection;
- Ensure that the recipients of the data are properly authorized people or Organizations and have adequate security policies;
- Report scams, privacy breaches and hacking attempts; and
- Avoid retaining files on desktop, all work files should be on shared folders.

General Security Instructions

To reduce the likelihood of security breaches, our organization will have all physical and digital shields to protect information, but the Organization also instructs all employees to:

- Keep a clean desk at all times;
- Turn off their screens and lock their devices when leaving their desks;
- Report stolen or damaged equipment as soon as possible;
- Change all account passwords at once when a device is stolen;
- Report threats or possible security weakness in the Organization systems; and
- Refrain from downloading suspicious, unauthorized, or unlicensed software on their equipment.
- Avoid accessing suspicious websites.

Remote Employees

Remote employees must follow this policy's instructions too. Since they will be accessing the Organization's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Data Control

As the Organization gathers and processes sensitive information, securing their data from unauthorized sharing and access should be the Organization's responsibility. To guard the confidential information shared inside and outside the Organization, all employees must:

- Refrain from sharing/transferring confidential data unless necessary;
- Use the or/ganization's private network when sharing sensitive data;
- Share data with authorized people and need credential to access;
- Limit file access only to the necessary people;
- Enable full-disk encryption before storing or sharing confidential data;
- Keep physical storage devices in the office;
- Delete outdated data and run through a file-shredder tool;
- Encrypt your physical and cloud backups to prevent any data leaks in case your backups are hacked;
- Have more than one copy of your data; and
- Review the data access list from time to time.
- Report suspicious emails or attempted cyber-attacks to investigate and resolve the issue immediately.

Network Access Policy

All employees are required to read and sign the Network Usage Policy, acknowledgement form, indicating receipt of, and understanding of their responsibilities.

Network includes, but is not limited to, Local Area Network (LAN), Wide Area Network (WAN), Internet, Intranet, telephone and wireless Communication access.

Chapter 4: Data Security and Protection

Internet Security Policy

- All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk.
- All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data is classified confidential. As per the below categories:-
    1. All session must pass through transparent proxy, except some categories such as banks, medical, healthy, er categories.
    2. High, and mid risk categories should be blocked and can’t be access at all.
    3. Low risk categories will appear a warning to worn the user and the user can go through the warning and access the site as long as he/she believe the site is not malicious
    4. New listed domain must be blocked and can’t be accessed

System Security Policy

- All systems connected to the Internet should have a vendor supported version of the operating system installed.
- All systems connected to the Internet must be current with security patches.
- System integrity checks of host and server systems housing high risk Caritas's data should be performed.

Chapter 4: Data Security and Protection

Data Security Guidelines:

- Identify and Categorize Data: Clearly distinguish sensitive information within the organization, particularly donor details, beneficiary data, and internal records.
- Access Management: Restrict access to sensitive data exclusively to authorized personnel, ensuring that staff members obtain access based on their specific roles and duties.
- Data Encryption: Apply encryption to sensitive data both during transit and while at rest, safeguarding it from unauthorized access, especially during information exchange with external partners or stakeholders.
- Secure Data Transmission: Utilize secure methods when transmitting sensitive data, especially in interactions with donors, partners, or other organizations.
- Regular Data Backups: Perform routine backups of sensitive data to mitigate the risk of loss in the event of system failures or data corruption, preserving the organization's ability to recover crucial information.
- Data Retention Guidelines: Establish and communicate guidelines on the duration for which various types of sensitive data should be retained, aligning with legal and ethical standards.
- Physical Security Measures: Enforce physical security measures to safeguard any physical copies of sensitive information, ensuring restricted access to documents or records.
- Secure Data Disposal: Set up secure procedures for discarding physical and digital records containing sensitive information, emphasizing responsible and ethical practices.
- Incident Response Strategy: Develop and regularly update an incident response plan specifically tailored to address potential data breaches, ensuring a prompt and efficient response to security incidents.
- Monitoring and Auditing: Deploy monitoring systems to trace access to sensitive data, conduct regular audits, and promptly address any unauthorized or suspicious activities.
- Password Protection Policies: Enforce robust password policies to secure access to databases and systems containing sensitive data, fostering a culture of secure password practices.
- Security for Remote Access: Implement secure measures for remote access, allowing staff to work outside the organization's premises securely while handling sensitive information.

- Data Security Culture: communication with personnel to enhance awareness and responsibility regarding data security among all members of the organization, emphasizing the significance of safeguarding sensitive information.

Chapter 5: Data Backup and Recovery

Section 1: Data Backup

Purpose of Backup:
The primary purpose of backup is to protect valuable organizational data from loss due to various factors such as hardware failure, data corruption, accidental deletion, or cybersecurity incidents.

Types of Backups:
Full Backup: A complete copy of all selected data.
Incremental Backup: Captures changes made since the last backup.
Differential Backup: Copies changes made since the last full backup.

Frequency of Backups:
Schedule backups based on the criticality of data, with more frequent backups for mission-critical information.

Storage Locations:
Onsite Backup: Store backups on servers or storage devices within the same physical location.
Offsite Backup: Maintain a copy of backups in an offsite location to protect against physical disasters.

Automated Backup Systems:
Automate the backup process with scheduled routines to ensure regular and consistent data protection. Implement automated checks to verify the integrity of backup files.

Encryption of Backup Data:
Encrypt backup files to safeguard sensitive information during storage and transmission.

Data Recovery:
The goal of data recovery is to restore lost or compromised data to its original state. Define the acceptable amount of data loss in case of an incident.

Disaster Recovery Plan:
Develop and maintain a comprehensive disaster recovery plan that outlines procedures for restoring data and systems after a catastrophic event.

Testing Backup and Recovery Procedures:
Conduct regular tests of backup and recovery procedures every 6 months to ensure the organization can quickly and effectively recover data when needed.

Documentation:
Document step-by-step procedures for both backup and recovery processes. Maintain an inventory of backup copies, including their locations and log.

Employee Training:
Train relevant staff on backup and recovery procedures, emphasizing their role in the event of data loss.

Monitoring and Auditing:
Implement monitoring systems to track backup activities and conduct periodic audits to ensure compliance.

Employee Responsibilities:
Communicate employee responsibilities in adhering to backup and recovery policies, including reporting any issues promptly.

Chapter 5: Data Backup and Recovery

Section 2: Testing Data Backup

Purpose of Testing Data Backup:
Ensure the reliability of our backup systems through periodic testing to ensure the backup and recovery process.

The IT Administrator is responsible for overseeing and conducting backup tests and collaborating with relevant teams for testing coordination.

Testing Procedure:

1. Backup Test Planning:

A) Clearly outline the goals of each backup test. That aims to validate the successful backup of critical data, test the restoration process, and ensure data integrity.
B) Determine specific scenarios to test, such as full system restores, partial restores, and application-specific restores.
C) Schedule tests during low-activity periods: Coordinate with relevant teams, considering operational needs, to schedule backup tests during periods of minimal impact on daily activities.

2. Backup Test Execution:

A) Select a diverse set of data to ensure a comprehensive test, covering various file types, sizes, and locations.
B) Execute the backup process using the established procedures, ensuring all relevant data is captured.
C) Documenting backup details: Record the start time, completion time, and any observations during the backup process.

3. Restore Test Execution:

A) Choose predefined scenarios, such as restoring a single file, a specific folder, or an entire system.
B) After the restore, validate the integrity of the restored data by comparing it with the original data.
C) Documenting restores details: Record the start time, completion time, and any issues or observations during the restore process.

4. Post-Test Verification:

A) Confirm system functionality: Collaborate with relevant teams, especially system administrators, to ensure that systems and applications are functioning correctly after the restore.
B) Checking backup and restore logs to identify any discrepancies, errors, or noteworthy observations.

5. Documentation and Reporting:

Summarize the results of the backup and restore tests, highlighting any issues encountered, provide a general overview of the test outcomes, suggestions for improvements based on the test results. This could include adjustments to backup schedules, additional training, or enhancements to backup procedures.

Chapter 5: Data Backup and Recovery

Section 3: Data Backup using One Drive

1. Setting Up OneDrive:
   a. Create a Microsoft account to serve as the primary access point for OneDrive.
   b. Download and install the OneDrive application from the official source onto the designated operating system.
   c. Authentication: Open the OneDrive application and authenticate it by entering the Microsoft account credentials.

2. Configuring OneDrive for Backup:
   a. Identify and manually select the folders and files to be backed up to OneDrive, including the option to back up standard folders such as Documents, Pictures, and Desktop.

   b. Setting Modifications: Access OneDrive settings to customize backup configurations, such as file synchronization, automatic uploads, and auto-start settings.

3. Working with OneDrive:
   a. Move or copy files into the designated OneDrive folder on the local device, ensuring synchronization with the OneDrive account.

   b. Access files remotely from any device by logging in to the OneDrive website or using the OneDrive app on mobile devices.

   c. Ensure that any modifications made to files within the local OneDrive folder are automatically synchronized with the corresponding OneDrive account.

4. Backup Management:
   a. Sync Status Monitoring: Regularly monitor the OneDrive icon in the system tray (Windows) or menu bar (macOS) to verify correct file synchronization and promptly address any issues.

b. Version Control: Utilize OneDrive's versioning feature to manage and restore previous file versions in case of unintended changes or deletions.

c. File Recovery: Restore deleted files from the OneDrive Recycle Bin within the specified timeframe for recovery.

d. Collaboration Guidelines: When sharing files, adhere to established guidelines to control access and ensure secure collaboration.

5. Security:

a. Two-Factor Authentication Activation: Enhance account security by enabling two-factor authentication through the designated settings.

b. Sharing Security Review: Regularly review and manage sharing settings to control access and maintain the security and privacy of stored data.

c. Device Management: Periodically review and manage devices connected to the OneDrive account to ensure authorized access.

Chapter 6: Anti-Malware and Antivirus

Virus Protection

All computers are equipped with Anti-Virus software. The software should be set to check all files before opening or executing them. The automatic virus update feature should be enabled on the computer. Do not turn this off.
If the employee encounters a virus on a computer, he/she must contact the IT Specialist immediately and leave the warning on the computer screen so that IT staff can see what they are dealing with otherwise take a screen shot and communicate it to the IT Specialist.

Virus Prevention Policy

- The willful introduction of computer viruses or disruptive/destructive programs into the Caritas's environment is prohibited, and violators may be subject to prosecution.
- All desktop systems that connect to the network must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor’s recommendations.
- All servers and workstations that connect to the network and that are vulnerable to virus or worm attack must be protected with an approved, licensed anti-virus software product that is kept updated according to the vendor’s recommendations.
- Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.
- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Guidelines:

- Choose a Good Antivirus: Use a reliable antivirus program on all computers and servers to protect against harmful files.

- Install and Update: Install the antivirus on all devices and keep it up to date for the latest protection.
- Regular Scans: Set up regular scans on devices to catch and remove any potential threats.
- Real-time Protection: Turn on real-time protection to stop viruses as soon as they're detected.
- Educate Employees: Train employees to recognize and avoid potential threats, promoting safe internet habits.
- USB and External Devices: Scan USB drives and external devices before connecting them to organization devices.
- Reporting Issues: Create a simple way for employees to report any suspected virus issues without fear of consequences.
- Incident Response Plan: Have a plan in place for dealing with virus incidents, including isolating affected systems and restoring data.
- Firewall Coordination: Coordinate antivirus efforts with the organization's firewall for extra security.
- Regular Checks: Conduct periodic checks to ensure the antivirus is doing its job effectively.
- Compliance: Make sure antivirus practices align with industry standards and regulations.
- Automated Fixes: Allow the antivirus to automatically fix issues to save time and effort.
- Quarantine Infected Devices: Isolate infected devices to prevent the virus from spreading.
- Document and Communicate: Clearly document antivirus guidelines and communicate them to all employees. Keep the information updated.

Chapter 7: IT Hardware and Equipment

Using IT hardware is for official tasks only. Keep passwords strong and confidential. Report issues promptly to the IT Specialist. Do not install unauthorized software or hardware. Protect sensitive information and follow security guidelines. Power off equipment when not in use.

Laptops/ Desktop Computer

Computers should be utilized exclusively for work-related purposes, and users are responsible for their security. Employees must not download or store sensitive data on personal devices and should report any loss or damage immediately. Regular backups of important files are essential to prevent data loss in case of unforeseen events. Full synchronization of data is to be made on the one drive of Caritas.

Printers

Printers are to be used for official documentation only. Individuals must refrain from unnecessary printing to conserve resources and ensure the efficient operation of printing equipment. Routine maintenance, such as replacing ink cartridges and promptly reporting malfunctions, should be performed to avoid disruptions in printing services.

Copiers

The copier is designated solely for official document duplication and printing purposes within the organization. Employees are expected to use the copier responsibly, avoiding unnecessary printing and ensuring that confidential information is handled securely during the copying process. Regular maintenance checks, such as clearing paper jams and replacing toner cartridges, should be carried out promptly to prevent disruptions in copying services. Additionally, employees should be mindful of energy conservation by turning off the copier when not in use. Any issues or malfunctions with the copier should be reported to the IT or administrative department immediately to ensure timely resolution and the continued smooth operation of this essential office equipment.

Scanners
Scanners are designated for scanning official documents, and users must exercise caution when handling delicate materials. The IT specialist should be notified promptly if any issues arise, and routine checks on scanner functionality should be conducted to maintain efficient document digitization processes.

Fax Machines
The fax machine is for official use only. Please send and receive work-related documents. Avoid personal use and ensure that sensitive information is sent securely. Regularly check paper and toner levels and report any issues to the IT or admin department promptly.

Projectors audio-visual equipment
Projectors and audio-visual equipment should be reserved for official presentations and meetings. Users must familiarize themselves with proper operation procedures to prevent damage and report any technical issues promptly. Ensuring that all equipment is turned off after use contributes to energy conservation and longevity.

Mobile Device Usage:
Mobile devices, if provided by the organization, are for work-related communication and tasks. Employees should adhere to security protocols, such as password protection and regular updates. Personal use of organization-provided mobile devices is strictly prohibited, and any loss or theft must be reported immediately to the IT specialist.

Server and Network Equipment Usage:
Access to servers and network equipment is only for authorized personnel. Use strong passwords, report issues to IT, and avoid unauthorized changes. If you notice anything unusual, let IT know. Don't install anything without permission.

Chapter 8: Cybersecurity Awareness:

1. Password Best Practices:
Complexity: Encourage employees to create strong passwords with a mix of letters, numbers, and symbols.
Avoid Sharing: Emphasize the importance of keeping passwords confidential and not sharing them with colleagues.

2. Phishing Awareness:
Recognizing Phishing: Train employees to identify common phishing attempts, including suspicious emails, links, and requests for sensitive information.
Verification: Stress the importance of verifying the legitimacy of unexpected emails before clicking on links or providing information.

3. Device Security:
Updates: Instruct employees to regularly update their devices with the latest security patches and software versions.
Screen Locking: Encourage the use of screen locks and password protection on devices to prevent unauthorized access.

4. Safe Internet Practices:
Secure Websites: Teach employees to look for "https://" in website URLs, especially when entering sensitive information.
Caution with Downloads: Advise against downloading files or software from untrusted sources.

5. Data Handling Guidelines:

emphasize the importance of handling sensitive data responsibly and securely.
Encryption: Introduce the concept of data encryption for an extra layer of protection.

6. Wi-Fi Security:
Encourage the use of secure, password-protected Wi-Fi networks, especially when working remotely. And advise against connecting to public Wi-Fi networks for work-related activities.

7. Two-Factor Authentication (2FA):
Implementation: Promote the use of two-factor authentication to add an extra layer of security to accounts.

8. Secure Email Practices:
Attachments and Links: Caution against opening email attachments or clicking on links from unknown or unexpected sources.
Email Encryption: Introduce the concept of encrypted emails for sending sensitive information.

10. Clean Desk Policy:
Confidentiality: Reinforce the importance of maintaining a clean desk, especially when dealing with confidential documents.
Securing Devices: Encourage employees to lock their computers when away from their desks.

11. Reporting Security Incidents:
Prompt Reporting: Establish a clear process for employees to report any suspected security incidents promptly.
No Retaliation: Ensure employees understand that reporting incidents will not result in retaliation.

12. Remote Work Security:
VPN Usage: Instruct employees on the use of virtual private networks (VPNs) for secure remote access.
Physical Environment: Emphasize the need for a secure physical workspace when working remotely.

13. Regular Training Updates: Schedule regular cybersecurity training sessions to keep employees informed about evolving threats and security best practices.

Chapter 9: Outsourcing IT Services

1. Planning and Assessment:
The Objective is to Clearly define the purpose and goals of outsourcing.

- Clearly outline the criteria of the outsourcing arrangement, specifying which IT services will be outsourced and the desired outcomes.
- Evaluate the organization's current IT capabilities and identify gaps or areas where outsourcing can provide value. Details the reasons for outsourcing, including potential cost savings, access to specialized skills, and improved efficiency.
- Identify potential risks associated with outsourcing, such as data security concerns or service interruptions, and develop strategies to mitigate these risks.

2. Vendor Selection:
Identify and select suitable IT service providers.

- Clearly define the criteria that will be used to evaluate potential vendors, including technical expertise, and financial cost.

- Prepare and distribute RFPs to potential vendors, outlining the organization's requirements, expectations, and evaluation criteria.
- Evaluate received proposals based on predetermined criteria. Conduct due diligence to verify references, review past performance, and assess financial stability.
- Based on evaluations and due diligence, choose the vendor that best aligns with the organization's needs and objectives.

3. Contracting:
Establish clear terms and conditions for the outsourcing agreement.

- Engage Legal and Procurement Teams: Collaborate with legal and procurement teams to negotiate contractual terms, ensuring legal compliance and protection of interests.
- Define Service Levels, Pricing, and Contract Duration: Clearly outline service levels, pricing structures, and the duration of the outsourcing contract.
- Agree on Security and Compliance Measures: Include provisions in the contract that address data security, compliance with relevant regulations, and any other legal considerations.

4. Transition Phase:
Plan a seamless transition of IT services from in-house to the outsourcing vendor.

- Develop a Detailed Transition Plan: Outline step-by-step procedures for transitioning services, including timelines, responsibilities, and milestones.
- Designate individuals who will be responsible for transferring knowledge and ensure a smooth transition.
- Define communication channels between the internal team and the outsourcing partner to facilitate a collaborative transition.

5. Governance and Management:
Establish a structure for overseeing and managing the outsourcing relationship.

- Clearly define the roles and responsibilities of both the internal team and the outsourcing partner.
- Set up effective communication channels to ensure regular updates, issue resolution, and coordination.
- Schedule regular meetings to review the progress of the outsourcing arrangement, address concerns, and discuss improvements.

6. Service Delivery and Performance Monitoring:
Ensure the outsourced IT services meet quality and performance standards.

- Establish Key Performance Indicators (KPIs) and Service Level Agreements (SLAs) to measure and monitor service quality.
- Use the defined KPIs and SLAs to regularly monitor and assess the performance of the outsourcing partner.
- Develop procedures for addressing any deviations from agreed-upon standards and expectations.

7. Communication and Reporting:
Establish clear communication channels and reporting mechanisms.

- Define communication protocols, channels, and frequency to maintain transparency and facilitate effective collaboration.
- Establish schedules for regular reporting on key performance indicators, project milestones, and any other relevant metrics.
- Clearly define procedures for escalating issues or concerns to ensure timely resolution.

8. Continuous Improvement:
Continuously enhance the outsourcing relationship and optimize processes.

- Schedule regular reviews to assess the effectiveness of the outsourcing arrangement and identify areas for improvement.
- Seek feedback from both internal stakeholders (Management and Staff) and the outsourcing vendor to gather insights and identify opportunities for enhancement.
- Use the feedback and insights gained to implement continuous improvement measures, adjusting processes and procedures as needed.

9. Contract Renewal or Termination:
Assessing the outsourcing arrangement and deciding on renewal or termination. By evaluating the outsourcing partner's performance against the objectives outlined in the contract.

Based on the performance review, decide whether to renew the contract, renegotiate terms, or explore alternative options.

If terminating the agreement, develop a plan for a smooth transition of services back in-house or to a new provider.