HUJRA
Village Support Organization

Information Technology (IT) Policy

Contents

Acknowledgment

We would like to extend our sincere appreciation to all employees, volunteers, contractors, and third-party users of Hujra Village Support Organization (HVSO) for their commitment to adhering to the IT Policy. Your dedication to responsible and secure IT practices is vital in supporting HVSO's mission of social and economic development.

We also acknowledge the invaluable contributions of the IT department in drafting, reviewing, and implementing the IT Policy. Your expertise and diligence ensure that HVSO's IT infrastructure remains resilient and aligned with best practices in information security.

Furthermore, we express gratitude to the leadership team of HVSO for their unwavering support of initiatives aimed at strengthening IT governance and safeguarding organizational assets.

Finally, we recognize the ongoing support and collaboration of our partners, donors, and stakeholders, whose collective efforts contribute to the success of HVSO's endeavors.

Together, we remain committed to upholding the principles outlined in the IT Policy, fostering a culture of responsible IT usage, and advancing the shared goals of social justice and sustainable development.

Thank you for your continued dedication and commitment to the mission of Hujra Village Support Organization.

1. Introduction:

The Hujra Village Support Organization (HVSO) recognizes the critical role of information technology (IT) in supporting its mission of social and economic development. As technology continues to evolve, it becomes increasingly important to establish clear guidelines and procedures to govern the responsible and secure use of IT resources within the organization.

The purpose of this IT Policy is to outline HVSO's expectations regarding the use of IT equipment, systems, and data to ensure confidentiality, integrity, and availability. By adhering to this policy, HVSO aims to mitigate risks, safeguard organizational assets, and foster a culture of responsible IT usage among its employees, volunteers, contractors, and third-party users.

This introduction serves as a preamble to the comprehensive IT Policy, which will address various aspects of IT governance, including email usage, internet browsing, administrative access, hardware service, security measures, data backups, and other computer-related activities. By establishing clear policies and procedures, HVSO endeavors to uphold its commitment to excellence, integrity, and transparency in all IT-related endeavors.

Through collaboration, accountability, and adherence to best practices, HVSO aims to leverage technology as a catalyst for positive change, empowering communities, and advancing its mission of social justice and sustainable development.

2. Policy Scope:

This IT Policy applies to all employees, volunteers, contractors, and third-party users who have access to Hujra Village Support Organization's (HVSO) IT resources. It encompasses all IT equipment, networks, systems, software, and data owned or managed by HVSO, regardless of the location from which they are accessed.

The scope of this policy extends to all IT-related activities conducted within HVSO premises, remote locations, or while using HVSO-provided equipment or services. It also applies to any IT-related activities conducted on behalf of HVSO, including those performed on personal devices if they access HVSO's networks, systems, or data.

This policy sets the standards and expectations for the responsible and secure use of IT resources to support HVSO's mission and objectives. It is imperative that all individuals covered by this policy understand and adhere to its provisions to ensure the confidentiality, integrity, and availability of HVSO's IT infrastructure and data assets.

HVSO reserves the right to enforce this policy and take appropriate action in cases of non-compliance, including disciplinary measures and legal recourse if necessary. By defining the scope of this policy, HVSO aims to create a secure and productive IT environment conducive to achieving its organizational goals and serving its beneficiaries effectively.

3. Acceptable Use

HVSO acknowledges the importance of IT resources in achieving its mission of social and economic development. Therefore, the acceptable use of these resources is vital to maintain efficiency, security, and integrity within the organization.

All users are expected to adhere to the following guidelines:

3.1. Authorized Use:

- HVSO's IT resources, including hardware, software, networks, and data, are provided for official business purposes related to the organization's mission and objectives.
- Limited personal use of IT resources is permitted, provided it does not interfere with work responsibilities or violate HVSO policies.
- Personal use must be conducted in a manner that upholds the organization's values and does not compromise the security or integrity of IT systems or data.

3.2. Prohibited Activities:

Users must refrain from engaging in the following activities:

- **Unauthorized access:** Users must not attempt to access IT systems, networks, or data without proper authorization.
- **Illegal activities:** Use of HVSO's IT resources for illegal purposes, including but not limited to hacking, distribution of copyrighted material, or engaging in criminal activities, is strictly prohibited.
- **Unauthorized disclosure:** Users must not disclose confidential or sensitive information without proper authorization, including HVSO's proprietary information, financial data, or personal information of employees, volunteers, or beneficiaries.
- **Malicious activities:** Introduction of malware, viruses, or other malicious software into HVSO's IT systems is prohibited.
- **Harm to reputation:** Users must refrain from engaging in activities that may damage HVSO's reputation or cause harm to its operations or stakeholders.

3.3. Monitoring and Enforcement:

- HVSO reserves the right to monitor and audit IT resource usage to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or legal consequences, depending on the severity of the violation and its impact on HVSO.

4. Data Security

Data security is paramount to Hujra Village Support Organization (HVSO) to safeguard sensitive information, maintain trust with stakeholders, and ensure compliance with legal and regulatory requirements.

The following measures outline HVSO's commitment to data security:

4.1. Confidentiality:

- All users are responsible for protecting the confidentiality of HVSO's data, including sensitive information related to beneficiaries, donors, partners, and organizational operations.
- Access to confidential data should be limited to authorized personnel with a legitimate need-to-know, and information should not be disclosed to unauthorized individuals or entities.

4.2. Data Protection:

- HVSO implements appropriate technical, administrative, and physical safeguards to protect data from unauthorized access, disclosure, alteration, or destruction.
- Encryption, access controls, and authentication mechanisms are employed to ensure data integrity and confidentiality, especially for sensitive or personally identifiable information.

4.3. Compliance:

- HVSO complies with relevant data protection laws, regulations, and industry standards governing the collection, storage, and processing of data, including but not limited to the General Data Protection Regulation (GDPR) and local data protection laws.
- Users must adhere to HVSO's data protection policies and procedures, ensuring compliance with legal requirements and organizational standards.

4.4. Incident Response:

- HVSO maintains an incident response plan to address data breaches, security incidents, or unauthorized access promptly and effectively.
- Users are required to report any suspected or actual security incidents to the designated IT personnel or management for investigation and remediation.

4.5. Training and Awareness:

- HVSO provides regular training and awareness programs to educate users about data security best practices, including password management, phishing awareness, and handling of sensitive information.
- All employees, volunteers, and contractors are required to undergo data security training upon joining HVSO and periodically thereafter to stay informed about evolving threats and mitigation strategies.

4.6. Data Retention and Disposal:

- HVSO establishes clear policies and procedures for the retention and disposal of data in accordance with legal requirements and organizational needs.
- Data that is no longer necessary for business or legal purposes should be securely deleted or disposed of to prevent unauthorized access or misuse.

4.7. Third-Party Data Handling:

- When engaging third-party vendors or service providers that handle HVSO's data, appropriate contracts and agreements are established to ensure compliance with data protection requirements and security standards.
- Third-party vendors must demonstrate a commitment to data security and adhere to HVSO's data handling policies and procedures.

5. IT Equipment and Software:

Effective management of IT equipment and software is essential for maintaining operational efficiency, productivity, and security within Hujra Village Support Organization (HVSO).

The following policies and procedures govern the acquisition, use, and maintenance of IT assets:

5.1. Authorized Use:

- Users must utilize IT equipment and software provided by HVSO for official work purposes in alignment with their job responsibilities.
- Personal use of IT equipment and software should be minimal and conducted in accordance with HVSO's acceptable use policy.

5.2. Software Licensing:

- HVSO ensures that all software used within the organization is properly licensed and legally acquired.
- Users are prohibited from installing or using unauthorized or pirated software on HVSO's IT equipment.

5.3. Equipment Allocation:

- IT equipment such as computers, laptops, mobile devices, and peripherals are allocated to users based on job roles and responsibilities.
- Requests for additional equipment or upgrades should be made through the designated IT support channels and approved by relevant stakeholders.

5.4. Equipment Maintenance:

- Users are responsible for the care and maintenance of assigned IT equipment, including regular cleaning, proper storage, and safe handling.
- Any malfunction or damage to IT equipment should be reported to the IT department promptly for assessment and repair.

5.5. Hardware Upgrades and Replacement:

- HVSO periodically assesses the performance and usability of IT hardware to identify opportunities for upgrades or replacement.
- Budgetary constraints, technological advancements, and organizational needs are considered when prioritizing hardware upgrades or replacements.

5.6. Software Installation and Updates:

- Installation of software on HVSO's IT equipment should be performed by authorized personnel following established procedures.
- Regular updates and patches for operating systems, applications, and security software should be applied to mitigate vulnerabilities and ensure optimal performance.

5.7. Remote Access:

- Remote access to HVSO's IT systems and resources is permitted for authorized users through secure and approved channels.
- Users must adhere to remote access policies and guidelines provided by the IT department to maintain the security and integrity of HVSO's network.

6. Network Security

Network security is paramount to Hujra Village Support Organization (HVSO) to safeguard against unauthorized access, data breaches, and cyber threats.

The following policies and measures are implemented to ensure the security and integrity of HVSO's network infrastructure:

6.1. Access Control:

- Access to HVSO's network resources is restricted to authorized personnel based on job roles and responsibilities.
- User authentication mechanisms such as passwords, biometrics, or access cards are employed to control access to networked systems and data.

6.2. Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS):

- Firewalls are implemented to monitor and control incoming and outgoing network traffic, filtering out unauthorized access attempts and malicious activities.
- Intrusion detection and prevention systems (IDS/IPS) are deployed to detect and mitigate suspicious or malicious network traffic in real-time.

6.3. Secure Wi-Fi Networks:

- Wireless networks within HVSO premises are secured using encryption protocols such as WPA2 or WPA3 to prevent unauthorized access.
- Access to Wi-Fi networks is restricted through the use of secure passwords or authentication methods to ensure only authorized users can connect.

6.4. Network Segmentation:

- HVSO's network is segmented to segregate different types of traffic and restrict access to sensitive systems or data.
- Segmentation helps contain potential security breaches and limit the impact of security incidents on critical network resources.

6.5. Virtual Private Network (VPN):

- VPN technology is utilized to provide secure remote access to HVSO's network resources for authorized users.
- VPN connections encrypt network traffic, ensuring confidentiality and integrity when accessing HVSO's network from external locations.

6.6. Regular Security Audits and Assessments:

- HVSO conducts periodic security audits and assessments of its network infrastructure to identify vulnerabilities, assess risks, and implement necessary security controls.
- Vulnerability scanning, penetration testing, and security assessments are performed by qualified professionals to maintain the security posture of HVSO's network.

6.7. Employee Awareness and Training:

- All employees, volunteers, and contractors receive training on network security best practices, including phishing awareness, password management, and safe internet browsing habits.
- Regular security awareness programs are conducted to keep users informed about emerging threats and cybersecurity trends.

7. Incident Reporting

Timely reporting and effective response to security incidents are crucial for mitigating risks, minimizing impact, and maintaining the security posture of Hujra Village Support Organization (HVSO). The following policies and procedures govern the reporting and management of security incidents:

7.1. Definition of Security Incidents:

- A security incident is defined as any event or activity that compromises or threatens the confidentiality, integrity, or availability of HVSO's IT systems, data, or network resources.
- Examples of security incidents include unauthorized access attempts, data breaches, malware infections, system outages, or suspicious network activity.

7.2. Reporting Process:

- All users who suspect or detect a security incident must report it immediately to the designated IT personnel or the IT department.
- Incident reports should include detailed information about the incident, including the date, time, nature of the incident, and any relevant evidence or observations.

7.3. Incident Response Team:

- HVSO establishes an incident response team comprised of qualified IT professionals responsible for investigating and responding to security incidents.
- The incident response team is trained and equipped to assess the severity of incidents, contain threats, and initiate appropriate remediation measures.

7.4. Incident Handling Procedures:

- Upon receiving a security incident report, the incident response team conducts a thorough investigation to determine the cause, scope, and impact of the incident.
- Based on the severity and nature of the incident, the incident response team initiates incident response procedures, which may include containment, eradication, and recovery efforts.

7.5. Communication and Notification:

- The incident response team communicates with relevant stakeholders, including senior management, IT staff, and affected parties, to provide updates and guidance throughout the incident response process.
- In the event of a significant security incident that may impact HVSO's operations or stakeholders, appropriate notifications are made to relevant authorities, regulatory bodies, or external partners as required by law or contractual obligations.

7.6. Documentation and Analysis:

- Comprehensive documentation of security incidents, including incident reports, investigation findings, and remediation actions, is maintained for analysis, auditing, and continuous improvement purposes.
- Post-incident analysis and lessons learned sessions are conducted to identify root causes, vulnerabilities, and areas for improvement in HVSO's security posture.

7.7. Training and Awareness:

- All employees, volunteers, and contractors receive training on incident reporting procedures, including how to recognize and report security incidents promptly.
- Regular security awareness programs and drills are conducted to ensure that users are prepared to respond effectively to security incidents.

8. Compliance

Compliance with relevant laws, regulations, standards, and organizational policies is essential for Hujra Village Support Organization (HVSO) to maintain trust, uphold ethical standards, and mitigate risks. The following policies and measures ensure compliance with applicable requirements:

8.1. Regulatory Compliance:

- HVSO adheres to all applicable laws, regulations, and industry standards governing its operations, including but not limited to data protection laws, privacy regulations, and financial reporting requirements.
- Compliance with regulatory requirements is monitored regularly, and necessary actions are taken to address any gaps or non-compliance.

8.2. Data Protection and Privacy:

- HVSO protects the privacy and confidentiality of personal data in accordance with applicable data protection laws and regulations, such as the General Data Protection Regulation (GDPR) and local data protection laws.
- Data protection policies and procedures are implemented to ensure that personal data is collected, processed, stored, and transferred securely and lawfully.

8.3. Security Standards:

- HVSO adopts industry-standard security practices and frameworks, such as ISO 27001, NIST Cybersecurity Framework, or CIS Controls, to establish a robust security posture and mitigate cybersecurity risks.
- Regular security assessments and audits are conducted to evaluate compliance with security standards and identify areas for improvement.

8.4. Ethical Standards:

- HVSO upholds high ethical standards in its operations, interactions with stakeholders, and use of IT resources.
- Employees, volunteers, and contractors are expected to conduct themselves ethically, with integrity, honesty, and respect for others, in accordance with HVSO's code of conduct and ethical guidelines.

8.5. IT Policies and Procedures:

- HVSO maintains comprehensive IT policies and procedures that outline expectations, guidelines, and best practices for the responsible and secure use of IT resources.
- Compliance with IT policies and procedures is mandatory for all users, and violations may result in disciplinary action or legal consequences.

8.6. Training and Awareness:

- HVSO provides regular training and awareness programs to educate employees, volunteers, and contractors about compliance requirements, ethical standards, and IT policies.
- Training sessions cover topics such as data protection, cybersecurity awareness, and regulatory compliance to ensure that users understand their responsibilities and obligations.

8.7. Monitoring and Enforcement:

- HVSO monitors compliance with policies, regulations, and standards through regular audits, assessments, and reviews.
- Non-compliance is addressed through appropriate enforcement measures, including corrective actions, training, and disciplinary measures, as necessary.

9. Policy Review

Regular review and updates of policies are essential for ensuring the effectiveness, relevance, and alignment of Hujra Village Support Organization's (HVSO) IT policies with evolving technology trends, organizational needs, and regulatory requirements.

The following procedures govern the periodic review and revision of IT policies:

9.1. Frequency of Reviews:

IT policies and procedures are subject to periodic reviews, which are conducted at least annually or more frequently as needed to address emerging risks, changes in technology, or regulatory updates.

9.2. Review Committee:

- A designated review committee comprising representatives from relevant departments, including IT, legal, compliance, and senior management, is responsible for overseeing policy reviews.
- The review committee ensures that policies are reviewed comprehensively, taking into account input from stakeholders across the organization.

9.3. Review Process:

- The review process begins with an assessment of the current policy's effectiveness, adequacy, and compliance with legal and regulatory requirements.
- Feedback and input are solicited from key stakeholders, including IT staff, department heads, and employees, to identify areas for improvement or updates.
- Proposed revisions or amendments to policies are reviewed and discussed by the review committee, considering factors such as emerging threats, technological advancements, and organizational priorities.
- The review committee collaborates to draft updated policy documents that incorporate feedback, address identified gaps, and align with best practices and industry standards.

9.4. Approval and Implementation:

- The revised policy documents are submitted for approval by senior management or the governing body of HVSO, according to the organizational structure and decision-making process.
- Once approved, the updated policies are communicated to all relevant stakeholders through appropriate channels, such as email notifications, staff meetings, or intranet announcements.
- Training sessions or awareness programs may be conducted to educate users about the changes to IT policies and procedures and ensure understanding and compliance.

9.5. Monitoring and Evaluation:

- Following the implementation of updated policies, ongoing monitoring and evaluation mechanisms are established to assess their effectiveness and adherence.

- Feedback from users and stakeholders is solicited to identify any issues or concerns related to the revised policies, and adjustments are made as necessary to address feedback and improve compliance.

9.6. Documentation and Recordkeeping:

- Comprehensive documentation of policy reviews, revisions, and approvals is maintained for accountability, transparency, and audit purposes.
- Records of policy reviews and updates are archived and accessible for reference during subsequent reviews or audits.