IIRR Global Information Technology Policy

Introduction

This Information Technology (IT) Policy establishes the framework for the effective, secure, and ethical use of IT resources within IIRR. As a globally distributed non-governmental organization with decentralized operations across multiple countries, the integrity, availability, and confidentiality of digital infrastructure are critical to IIRR's mission of rural reconstruction.

This policy aims to safeguard the organization's data, systems, personnel, and beneficiaries by defining the roles, responsibilities, and acceptable behaviors in managing technology. It applies to all staff, including employees, interns, contractors, consultants, volunteers, and any third parties who have access to the organization's digital assets.

Objectives

The primary objective of this policy is to ensure that all IT systems and resources are used in a secure, efficient, and responsible manner that supports the organization's operational and strategic goals. It also aims to establish clear protocols for mitigating security threats, promoting cybersecurity awareness, standardizing IT practices across field offices, and ensuring compliance with international data protection laws and donor requirements.

Scope and Applicability

This policy applies to all offices, departments, and affiliates of IIRR, regardless of geographic location. It encompasses all physical and virtual IT assets including but not limited to laptops, desktops, mobile devices, servers, storage systems, cloud platforms, communication tools, software applications, and data repositories. It governs access to both on-premise and remote IT environments and applies equally to staff working in headquarters, regional hubs, country offices, and field locations.

IT Governance and Structure

IIRR's Headquarters is responsible for defining the strategic direction, standards, and policies for IT infrastructure and cybersecurity across the organization; primary responsibility for this function is assigned to the Director of Global Operations.

Each regional or country office must designate an IT focal point responsible for implementing and enforcing this policy locally, while ensuring alignment with global IT protocols. IT decisions, especially those involving procurement, infrastructure changes, cloud adoption, or major digital initiatives, must be made in consultation with Headquarters to ensure interoperability, compliance, and cost-efficiency.

Acceptable Use of IT Systems

All IT resources must be used in a manner that is ethical, legal, and consistent with the organization's values and operational priorities. IT systems are primarily intended for professional use. Reasonable personal use is tolerated as long as it does not interfere with productivity, consume excessive bandwidth or resources, or introduce security vulnerabilities. Users are strictly prohibited from using organizational IT resources for illegal, discriminatory, or malicious activities.

The use of unlicensed software, unauthorized devices, or peer-to-peer file sharing on organizational networks is not allowed. All users are expected to adhere to professional digital communication standards and avoid any actions that may damage the organization's reputation or security posture.

Mitigating IT and Cybersecurity Threats

Given the global nature and humanitarian focus of IIRR, the organization is frequently a target for sophisticated cyberattacks, including phishing, ransomware, data breaches, and social engineering campaigns. As such, proactive measures are required to mitigate these risks. The organization will develop a centralized cybersecurity strategy, guided by international best practices and standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework. All systems must be configured according to secure baseline standards approved by the Global Headquarters. Antivirus and endpoint detection software must be installed and regularly updated on all devices. Firewalls, intrusion detection systems (IDS), and secure access controls must be employed on networks and critical applications.

To mitigate human error—the most common source of cybersecurity incidents—all staff will be required to undergo regular cybersecurity training. These training programs cover phishing awareness, secure password practices, mobile device safety, and data handling protocols. Any suspicious emails, attachments, or links must be reported immediately to the local IT focal point for investigation, with escalation to Headquarters as needed.

In addition, security threat assessments will be conducted periodically at both global and local levels. Penetration testing, vulnerability scans, and incident response simulations will be organized to test resilience and identify weaknesses. Offices must also implement secure network configurations, including VPN usage for all remote access and multifactor authentication for all sensitive systems.

Data Protection and Privacy

All data managed by IIRR, whether related to program participants, donors, staff, or partners, must be handled with the utmost confidentiality and integrity. Personal data must be collected and processed lawfully, transparently, and for defined purposes only. The organization complies with relevant data protection laws including the EU General Data Protection Regulation (GDPR), as well as applicable national laws in countries of operation. Personal data must be stored

securely and access must be restricted based on job roles and operational necessity. Data encryption is mandatory for both data at rest and in transit.

Staff must not store sensitive data on personal devices or unapproved cloud platforms. When using portable media or mobile storage devices, encryption and password protection must be applied. In cases where data must be shared externally, it should be anonymized or pseudonymized where possible, and subject to formal data-sharing agreements. Retention periods for various data types are defined in the organization's Data Management Policy, and data must be deleted or archived securely once those periods expire.

Access Control and Authentication

To ensure that only authorized individuals can access the organization's digital resources, strict access control mechanisms must be implemented across all systems. Every user must have a unique ID and password, and account privileges must be assigned based on the principle of least privilege. Administrative accounts must be closely monitored and should not be used for routine activities. Passwords must meet complexity requirements set by the Global Headquarters and be changed at regular intervals. Multifactor authentication (MFA) is required for email, remote access, and cloud platforms. Shared accounts are discouraged; where unavoidable, shared credentials must be stored securely and access logs maintained.

Network Security and Internet Use

All office networks must be secured through the use of firewalls, updated firmware, segmented subnets, and strong Wi-Fi encryption protocols such as WPA3. Public or unsecured networks must not be used for transmitting sensitive data unless a VPN is used. Internet use must be responsible and aligned with operational needs. Streaming services, social media, and personal downloads that consume significant bandwidth are restricted unless justified for work purposes. Offices with limited internet connectivity must prioritize essential communication and programmatic activities.

Cloud Computing and Data Storage

The organization uses cloud services for data storage, email, file sharing, and productivity tools to enhance global collaboration and operational efficiency. All cloud providers must meet internationally recognized security standards and provide data residency guarantees where required. Staff are prohibited from using unauthorized or personal cloud services for storing or sharing work-related data.

The Global Headquarters retains administrative control over all cloud platforms and is responsible for configuring security settings, managing user permissions, and monitoring activity logs. Automated backups, redundancy, and access controls are enforced to prevent data loss or unauthorized access.

Email, Communication, and Collaboration Tools

Email is the official mode of communication for all organizational activities. All users must use their IIRR email addresses for work-related correspondence. Auto-forwarding of emails to personal accounts is prohibited. Users must remain vigilant to phishing attempts and avoid clicking on suspicious links or attachments. Collaboration platforms such as Teams, Zoom, Google Workspace, and similar tools must be pre-approved by the local IT focal point. All official communication must adhere to professional standards and be archived where necessary to meet documentation and compliance obligations.

File Sharing through Google Drive

To protect the organization's data, ensure accountability, and maintain compliance with data protection standards, all staff, interns, consultants, and partners are required to access and share Google Drive files using their official IIRR email accounts (e.g., @iirr.org).

Opening or requesting access to organizational Google Drive links from personal email accounts (e.g., Gmail, Yahoo, Outlook) is not allowed. Users may not share internal documents from Drive to personal or unverified external accounts without explicit authorization from the local IT focal point.

When collaboration with external partners is required, access will be granted to verified external addresses as approved by the user's supervisor or local IT focal point. Always use "view-only" or "comment-only" permissions unless editing rights are necessary.

Device and Software Management

All hardware and software used in the organization must be approved and centrally managed by the local IT focal point. Only authorized devices may connect to the organization's networks. Users are prohibited from installing unauthorized software or applications that have not been appropriately vetted. Regular software updates and security patches must be applied to all systems to protect against known vulnerabilities. Mobile devices used for work purposes must have passcodes, remote wipe capabilities, and management software installed. Lost or stolen devices must be reported immediately to the local IT focal point, and appropriate actions will be taken to protect data.

Backup and Disaster Recovery

To protect against data loss, the organization maintains a rigorous backup and disaster recovery strategy. All critical systems and data are backed up regularly using automated processes. Backups are encrypted and stored in geographically diverse and secure locations. Offices must ensure compliance with the backup schedules set by the IT Department. Disaster recovery plans must be reviewed and tested regularly to ensure preparedness in the event of cyberattacks, natural disasters, system failures, or geopolitical disruptions.

Incident Management and Reporting

A formal Incident Response Plan (IRP) is in place to guide the organization in responding to cybersecurity incidents, system outages, and data breaches. All staff must report suspected incidents immediately through designated reporting channels. The Global Headquarters will coordinate with local IT focal points to investigate, contain, and remediate incidents, and to notify stakeholders and regulators when required. All incidents are logged, documented, and analyzed for future prevention. Failure to report an incident in a timely manner may result in disciplinary action.

IT Capacity Building and Awareness

Recognizing that staff behavior is often the first line of defense against cyber threats, IIRR invests in regular training and awareness campaigns for all personnel. Onboarding processes must include IT orientation and basic cybersecurity training. Annual refresher courses are mandatory for all staff. Specialized training is provided for IT personnel and staff with access to sensitive systems. The organization encourages a culture of vigilance, where users are empowered to question suspicious activity and prioritize cybersecurity.

Compliance, Monitoring, and Audit

The organization reserves the right to monitor its IT systems, networks, and usage logs in accordance with local laws and global privacy standards. This monitoring is necessary to ensure policy compliance, detect unauthorized activities, and protect organizational assets. Periodic internal and external IT audits will be conducted to evaluate policy adherence, identify gaps, and improve system resilience. Staff found to be in violation of this policy may face disciplinary action, including access restrictions, formal reprimands, or termination, depending on the severity of the breach.

Policy Review and Revision

This policy is subject to annual review by the Global Headquarters in coordination with the Legal, Compliance, and Human Resources advisors. The policy may be updated more frequently in response to significant changes in the threat landscape, legal requirements, or organizational strategy. All changes must be communicated organization-wide and acknowledged by staff through appropriate training and policy sign-off mechanisms. Local adaptations of this policy must align with the global standard unless superseded by mandatory local law.

Conclusion

The security and efficiency of IT systems are foundational to IIRR's ability to deliver on its mission. This policy serves as a unified global standard for responsible IT management, operational resilience, and cybersecurity preparedness. Every staff member, regardless of

location or role, shares responsibility for safeguarding the organization's digital environment and upholding the principles outlined in this document. Compliance with this policy ensures the protection of sensitive data, the continuity of operations, and the trust of IIRR's beneficiaries, donors, and partners worldwide.

Last update: December 2, 2025