Title:	**IT policy**
Policy statement:	DSPR is committed to maintaining the highest standards in IT for the best service towards its local partners and communities; therefore, as part of our mandate, an electronic environment that encourages the use of computers and electronic communications as essential tools to support its mission and for effective administration. All of DSPR's provided software, and hardware, IT equipment remains the property of DSPR and must be used responsibly. The downloading and installation of applications, programs, and non-work-related software, etc., is not permitted. Therefore, use of IT resources that must be used for official organizational business only. Personal use of IT assets should be minimal and must not interfere with work responsibilities. Furthermore, only authorized IT personnel may repair or upgrade hardware. Any security incidents, data breaches, or IT malfunctions must be reported to the line manager immediately in order to acquire IT support (staff or third-party providers) to assist with troubleshooting and ensuring compliance with IT policies. Software licensing agreements must be adhered to, and piracy is strictly prohibited. On Data Security and Confidentiality - All staff, volunteers, must do their utmost to protect the data and confidentiality of information where it applies; they are also strongly encouraged to use strong passwords and change them regularly. - Sensitive data must be stored securely and accessed only by the respective authorized personnel. Confidential information must not be shared via email or external storage without proper encryption. Where possible, staff are encouraged to conduct multi-factor authentication (MFA) to access systems. - The organizational local hard drives of a workstation should not be used to store documents as files stored on local drives are not backed up and cannot be recovered in the event of a deletion or hard disk failure. Consequently, all files or documents located on the C: and D: drive are the responsibility of the user. - Any information stored on DSPR's systems is considered as professional property, and consequently, the property of the organization. Users storing information on the organizations' drives e.g. F,G,H of the network, should do so responsibly. F drive is the user's personal drive, accessible only to the individual user and authorized LAN administrators. Programs should not be stored or installed on F: drives. When requested by the supervisor, the data can be transferred to another person in case it is necessary for the continuity of the work. If the information stored is private, it should be stored in a folder clearly labelled "Private". The fact that the owner's name is mentioned in the file name is not sufficient to make it private. As for H: & G: drives, these are organizational and departmental drives, providing a common area where users can share data and files. Programs should not be stored or installed on H:\ & G:\ drives. Documents located on H: & G: should be organized to avoid duplication and to allow unused files to be easily moved or deleted. - For confidentiality reasons, DSPR will not monitor staff behavior in electronic communications. However, basic and anonymous information is logged and could be

investigated, if required for organizational needs within the legal framework, or could be surrendered on judicial order.

On the Internet & Email Usage

- DSPR's internet and email systems must be used responsibly and professionally. Accessing or distributing offensive, illegal, or harmful content is strictly prohibited. Email attachments should be scanned for viruses before opening.
- Staff, volunteers, visitors of staff granted access to the Internet are required to use their access in a legal, responsible and informed manner conforming fully to network etiquette, customs and courtesies. They should be well aware that the internet is not a fully secure channel and should not be used for sending or receiving sensitive information.
- (Visitors log-in for the office network)
- Any willful misuse of the internet by any employee may result in disciplinary action, including, but not limited to, termination of employment. Examples of unacceptable conduct include but are not limited to use of offensive or abusive language either in public or private messages, unlawful activities, defamation, infringement of copyrights, and misrepresentation of oneself.
- It is strictly forbidden to access illegal internet sites and or to save any offensive files, images, etc., on any drive, or to forward them. Copyrighted material for which users do not have authorization or permission must be respected.

Emails

- A DSPR email account will be provided to staff for work use within one week of their induction to the organization. This account will be frozen when a person is no longer working for the organization. The employee's mailbox is kept for one month after the announced departure date to allow an eventual transfer of data stored in the user mailbox. On request by the supervisor, the data can be transferred to another person to guarantee the continuity of the work.
- The email system in place is a personal system, unless a delegation is set up by its owner, or requested by the supervisor. As the email system is devoted to professional use, the content of a user mailbox is the property of his/her employer and the employer can, upon formal management decision communicated to the technician, break the confidentiality of the mailbox by clearing the user-assigned mailbox password.
- Personal use is authorized, if it is minimal, and does not affect work adversely. Users must identify themselves with their full email address and legal name. DSPR neither assumes nor shares responsibility for incidents of harassment, slander, malice, defamation of character, copyright violations, or any civil or criminal actions that occur or are alleged to have occurred through any personal or inappropriate use of email. The responsibility is solely that of the individual.

Procedures:	The scope of these procedures for enforcing the organization's IT policy, ensuring secure, efficient, and ethical use of IT and other technological resources. For more details, see Annex 1: IT Policy Procedures. Annex 2: Awareness, Training and Orientation Materials on IT (PowerPoint) and other materials.
Definitions:	**Local drives**: storage devices physically located on your computer, such as the **C:** drive or **D:** drive. These drives store files, programs, and system data locally on the machine and are only accessible from that specific device unless shared. **Backup system**: is a method or service used to create copies of data to protect against loss, damage, or corruption. It can include external hard drives, cloud-based services, or automated software that schedules regular backups. **Network drives:** are shared storage areas located on a central server within an organization's network. They are mapped to a drive letter (e.g., **F:** or **G:**) and allow multiple users to access shared files and folders Internet **Internet**: is a global network of interconnected computers that enables the sharing of information and services such as websites, cloud storage, communication, and remote access tools. **Email accounts**: are digital mailboxes that allow users to send, receive, and store electronic messages and files. They can be personal (e.g., Gmail, Yahoo) or work-related (e.g., Outlook, company domain emails). DSPR has its own domain. **Social media**: refers to online platforms that allow users to create, share, and interact with content and each other. Organizations may use social media for marketing, communication, or beneficiary support.
Related Policies & Procedures:	- Code of conduct - Safeguarding Policy - Communication and branding policy
Why is the policy needed:	The secure all communication department and archive; to avoid of any data misuse.
Who must follow this policy:	All staff, volunteers, consultants and third parties who access DSPR's IT resources including hardware, software, networks and data must follow this policy.

Next formal review:	Next review and approval date within 3 years of the above date or sooner if legislation, best

	practice or other circumstances indicate that it is necessary; **May 2028**
Person responsible:	DSPR Executive Director AC Executive Directors
Version:	11 June 2025
Approved by:	Central Committee Members: Dr. Audeh Butros Audeh Quawas; Chairperson-Member at Large- Representing Orthodox Church Family Mr. Bassem Issa Audeh Thabet Vice- Chair- Delegate DSPR-ICC Jerusalem & WB Area Committee Dr. Farah Atallah Farah Attallah; Treasurer- Delegate DSPR-NECC Jordan Area Committee Bishop Sani Ibrahim Charly Azar; Member at Large- Representing Episcopal – Lutheran Church Family Mrs. Sandra Tawfiq Habesch Khoury; Member at Large- Representing Catholic Church Family Dr. Jean Salaminian; Member at Large- Representing Eastern Orthodox Church Family Mr. George Jamal Jamil Antone; Delegate DSPR-NECC Gaza Area Committee Mr. Adel Nasser; Delegate DSPR-ICCI Galilee Area Committee MS. Nina Farah Shaddad; Delegate DSPR-JCC Lebanon Area Committee
Approval date:	Central committee meeting: 4 July 2025

Annex 1: IT Policy Procedures

Staffing

- IT Staff to build up a Local Net Work (LAN) for all the offices and a secured VPN access for the staff. The IT staff will be responsible to install a mini program on the main servers to remind the staff to change their passwords periodically.
- Should we not have such a staff we need to contract a computer company to perform such duties.
- In case of non-availability of an IT services we suggest that the authority of the passwords file be given to follow up on creating and deleting passwords for new / leaving staff or user. A written request needs to be submitted counter signed by the executive director.

Device Management

- Asset Registration: All IT hardware and software must be registered in the asset inventory system.
- Endpoint Security: All devices must have approved antivirus and protection.
- Remote Access: Remote access is allowed only via secure VPN with multi-factor authentication.

Software Installation

- Licensed Software Use:Only licensed software is permitted. Pirated or unauthorized software is strictly prohibited.

Data Protection

- Data Classification: Data must be classified as Public, Internal, Confidential, or Restricted.
- Backups: Daily backups must be performed and verified. Monthly backups should be stored offsite or in secure cloud storage.

Network Security

- Firewall & Intrusion Detection: Firewalls and IDS must be configured and monitored regularly.
- Network Segmentation: Separate networks for guest users, employees, and critical systems.

Incident Response

- Reporting: All IT incidents (e.g., malware, data breaches) must be reported to the executive directors within one hour.
- Post-Incident Review: Conduct a root cause analysis and update controls as needed.

IT Acceptable Use

- Personal Use: Limited personal use of IT resources is permitted, provided it does not interfere with work.
- Prohibited Activities: No use of IT resources for illegal, harassing, or unauthorized commercial activities.

Annex 2: Awareness, Training and Orientation Materials on IT (PowerPoint) and other materials