

IT Security & Data Protection policy

Version: 2.0

Policy Owner: Finance & Administration Director

Endorsed by Mission East Board

Applicable

Contents

Background & Context.....	1
Policy	1
1 Scope & applicability.....	1
2 Definitions.....	2
3 Purpose.....	2
4 Provisions	3
5 Related documents.....	4
5.1 Related Policies	4
5.2 Related SOP and guidelines.....	4
6 Responsibilities	4
7 Review.....	5

Background & Context

The past decade has shown number of IT security breaches and personal information leaks in all sectors, leading to suspension of operations or personal attacks. Furthermore, Mission East recognises that it operates in regions where powerful actors may be interested in harming our IT system or getting access to our data – organisational or personal – to limit or harm our operations, our staff or the people we work for and with.

Mission East is committed to its Accountability & Performance policy and the EU General Data Protection Regulation ([2016-679](#)) and considers that IT infrastructure security and data protection are crucial to maintain its business continuity and to not harm individuals.

This policy sets a frame to ensure the necessary IT infrastructure security and data protection.

Policy

1 Scope & applicability

- 1 This policy applies to all Mission East staff (including all employees, interns, volunteers and board members), temporary agency workers and consultants, who are working or are on mission for Mission East, **wherever they may be based**¹ and whatever type of data they process.
- 2 In addition, the Purpose and Provisions outlined herein are extended to apply to all those who work in partnership with Mission East or those who are contracted to provide services to the organisation.
- 3 The individuals and organisation members mentioned above will be referred to herein as “**Staff**”, independently of their level in the hierarchy or relationship with Mission East.
- 4 Data refers in this policy and related SOP to both Organisational Data and Personal Data, stored and processed either electronically or not (paper/hard copy).

¹ Personal Data related to people based in Europe, or people outside Europe whose personal information comes from or to Europe, are covered by the GDPR. As Mission East’s IT infrastructure is based in EU countries, all Personal Data that are electronically managed are under the EU General Data Protection Regulation independently on the location of the Data Subject or Data Processor.

- 5 This policy will come into effect from the date of its publication on Mission East digital Staff Handbook and will stay applicable without any other limit of time than the endorsement of a newer version.
- 6 If the legislation in the Data Subject's country of residence or the Staff's country of employment defines other rights and obligations than those given by the terms of this policy and is more restrictive than the European GDPR, then the relevant national legislation will take precedence over Mission East policy.
- 7 Any behaviour and action will be assessed in accordance with this policy during its period of application. Failure to comply may lead to further formal action, up to and including the termination of any contract, agreement or engagement with the organisation in accordance with Mission East's Discipline policy.

2 Definitions

For this policy and all related documents including related policies and SOPs, the following definitions apply.

- 1 **Availability** means that authorised users should be able to access data if they need it for authorised purposes.
- 2 **Integrity** means that data should be accurate and suitable for the purpose for which it is processed.
- 3 **Confidentiality** means that information will not be disclosed to any other person than the Data Subject or the Data Users.
- 4 **End-to-End IT Security** covers protection and risk mitigation measures at all data transfer and management steps from the provider of the data to the IT systems, servers and network to the end-user.
- 5 **Personal Data** is defined by the European GDPR as all kind of information upon a person which alone or combined can lead to the identification of a physical person, disregard of the way data is stored and processed (electronically or not). We consider generally three types of Personal Data:
- 5.1 **Public Data** is any information that can be made freely accessible by anyone or is already (e.g., social media, public records, press releases, and promotional materials). These data can be collected and processed without consent as long as there are used in accordance with the purpose of their original publication, and the Data Subject is informed of the source we have used to collect them.
- 5.2 **Confidential Data** is any personal information that is neither public nor sensitive. Such data requires elevated access permissions and often the Data Subject's consent. Bank account, family relationships, private phone number and e-mail are example of such data. These data should be restricted with role-based access rights and shouldn't be shared outside the organisation unless the recipients have been granted those same access rights, and the Data Subject has been made aware of data sharing.
- 5.3 **Sensitive Data** revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a physical person, data concerning health or data concerning a natural person's sex life or sexual orientation. Such data may only be collected if absolutely required and with the Data Subject's informed consent.
- 6 **Organisational Data** covers all data that are not classified as Personal Data which are necessary for Mission East's operation and management. It includes but is not limited to financial, strategic, programmatic, monitoring, evaluation and lessons learned data. Organisational data are considered as confidential.
- 7 **Data Subject** is the owner of Personal Data: the individual who can be identified behind data content.
- 8 **Data Controller** is defined by the European GDPR as the physical or legal identity, authority, institution or other organisation which alone or together with other, defines the purpose and the mean for gathering Personal Data. Mission East is the Data Controller of all personal data held on staff, supporters, local partners, donors, recipient of marketing activities, third parties and other contacts used for our activities.
- 9 **Data Processor** is defined by the European GDPR as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Mission East uses Data Processor for example to administrate IT systems and digital communication tools or engages with partners to implement projects.
- 10 **Authorised Users** or **Data Users** are Staff who need access to information to complete the tasks they are assigned to fulfil the purpose of their role.
- 11 **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

3 Purpose

This policy outlines Mission East's commitment and approach to preventing breaches of IT infrastructure and personal data confidentiality. It establishes provisions that all Mission East staff, as defined above, must uphold to:

- 1 Ensure that Mission East's IT systems are easily available to Staff and are maintained with the purpose of high Integrity and Confidentiality.
- 2 Staff understand their responsibility in contributing to a safe IT infrastructure and the protection of Personal Data, how to behave accordingly and lawfully, fairly and in a transparent manner in relation to the Data Subject.
- 3 Data Subjects know their right and how they can report any concerns related to their Personal Data.
- 4 Ensure that effective, safe, and accessible feedback and response systems are in place to report any suspicions of Personal Data breach or misuse.

This policy outlines Mission East's commitment and approach to upholding the rights and dignity of all, including children, adults at risk, affected populations, staff, partners and all Mission East's stakeholders.

4 Provisions

All Staff (defined in chapter 1 paragraph 3) are committed to the following provisions.

- 1 **Mission East:**
 - 1.1 Develop, implement and maintain an operational management system framework for information security (ISMS), including procedures and guidelines for handling Mission East End-to-End IT security and Data Protection that corresponds to best practice as described in the international standard ISO/IEC 27002.
 - 1.2 Engage 1) Data Processor Agreement with all its subcontractors who manage Personal Data under the responsibility of Mission East, and 2) Data Transfer Agreements with stakeholders outside the European Economic Area (EEA), as soon as there is an exchange of Personal Data between the parties.
 - 1.3 Is committed to train and supervise Staff so they understand their commitment with regard to this policy and related SOPs as well as the behaviour expected of them.
 - 1.4 Supports local partners in applying this policy as a best practice guide when collecting, storing, and using personal and sensitive information.
 - 1.5 Appoint a Data Privacy Team who has day to day responsibility for all data protection and legal compliance at global and HQ levels.
 - 1.6 Maintain registers of data processing activities, data processors, suspected or confirmed data breach, and report any breach in accordance with the European GDPR.
 - 1.7 Will not access information in Staff e-mails, personal cloud, hard disk or back-up or other electronic support unless it is required for security reasons or by a Complaint investigation team.
- 2 **Mission East's Secretary General, Directors and Managers must:**
 - 2.1 Onboard all new staff, so they receive orientation on this Policy and related SOPs and on the proper data processing procedures aligned with the register of data processing activities.
 - 2.2 Organise work so their teams are provided adequate resources to maintain compliance. Resources include skills training and time allocation for regular updates to the data processing register, proper communication with Data Subjects and efficient management of Data Subject requests.
- 3 **Staff** are committed to supporting IT security and Personal Data protection and must:
 - 3.1 Secure all devices which can be used to access Mission East data (Mission East's or own device) according to IT Users SOP including:
 - Using strong, unique passwords and keep systems updated
 - Preventing theft and unauthorized access
 - Avoiding unapproved sites, apps, or platforms as defined by the SOP
 - 3.2 Actively protect data e.g.:
 - Lock all data from unauthorized third parties
 - Prevent confidential information from being visible to unauthorized individuals
 - Store data only in Mission East authorized storage systems
 - 3.3 Follow the data collection and processing nearly described in practice in IT Personal Data Management SOP including:
 - Follow "Need-to-Know" and "Do-No-Harm" principles: collect only necessary data, ensuring that data processing will not put the Data Subject at risk.
 - Process data fairly and lawfully in compliance with GDPR
 - Design processes for optimal privacy protection
 - Inform subjects about data collection purposes and their rights
 - Delete or pseudonymize data upon request or when no longer needed
 - 3.4 Report any data breach concerns immediately to data_breach@missioneast.org

- 4 **Staff and all those who work with or for Mission East** are not allowed to access unauthorized websites, cloud storage nor use USB devices without special permission. This limitation is merely defined in the IT Users SOP
- 5 **All other entities who work with Mission East** will be expected to protect Personal Data in accordance with this policy.

5 Related documents

Mission East's Code of Conduct summarises the main expectations to Staff behaviours. All documents listed below relate closely to the present Policy and define concomitant Staff obligations.

5.1 Related Policies

- Accountability & Performance policy and Protection from SEAH and Child Safeguarding policy
- Discipline policy

5.2 Related SOP and guidelines

- IT Users SOP and IT Infrastructure & Security Management SOP
- Personal Data Management SOP
- Complaint Reporting & Case Management SOP

6 Responsibilities

The **Board** of Mission East has the ultimate accountability for this policy including its compliance to the international standards, Mission East is committed to, its endorsement, and its implementation across all aspects of the organisation's work by holding the Secretary General accountable to how effectively this policy is implemented.

The **Secretary General** is responsible for ensuring that this policy is upheld including ensuring the necessary resources and procedures to do so. The Secretary General must inform the Board of any concerns relating to complaints that may present risk to Mission East or its staff and give regular progress reports to the Board.

All Managers, independently of their hierarchical level, including the Secretary General, are responsible to demonstrate their commitment to this policy and:

- Lead by example and complies with this policy.
- Foster a culture that support their staff commitment including staff understanding of the policy purpose and provisions, the related procedures, the expectations they must meet and their responsibilities.
- Report to their Manager any concern related to the implementation of this policy.
- Monitor and respond to any complaint that is assigned to them to investigate.

Programme Managers (HQs) and Country Directors are also responsible for communicating this policy and related procedures to staff, local partners and others who use Mission East's IT system or manage Personal Data for Mission East, ensuring that Data Processor or Data Transfer Agreements are in place when necessary.

All staff whatever their level in the hierarchy or relationship with Mission East are responsible for:

- Understanding and following this policy and related procedures, incl. the eventual updates, and ensuring that their individual actions and behaviour are in line with this policy.
- Supporting other staff to comply to this policy and related procedures and a culture that foster this policy and its purpose.
- Not encouraging others (directly or indirectly) to breach this policy; this will be considered as a serious breach of commitment.
- Reporting any breaches in the provisions of this policy or related procedures in accordance with the Reporting & Case Management SOP.

IT Managers are responsible for developing, maintaining and implementing IT infrastructure, systems and standards that support this policy and which are in accordance with international and local laws and best practices. There are also for responsible for reporting of data breach and the maintenance of Data Processors and Data breach registers.

Data Privacy Team members are responsible for supporting their team in the implementation of this policy and related SOPs in day-to-day operations, identifying needs to review them, updating the register of data processing activities, and generally monitoring Mission East internal compliance.

HR Director is responsible for developing and maintaining training material and supporting Directors in staff understanding of this policy.

7 Review

The next review will take place before end of 2028 or at any time as required by major changes in Mission East's organisational set up, strategy or context that makes the current version flawed, partially outdated or obsolete.

It is the responsibility of the Policy Owner to ensure the revision in accordance with the above.