INFORMATION SECURITY POLICY

Approved on:	2019-April-10
Approved by:	Executive Board
Version:	1
Created by:	Information Technology
Next review:	2024
Point of contact:	Linda Szelag Head of Information Technology T: +49 (0) 228 2288105 IT@welthungerhilfe.de

Binding for:

- All employees of Welthungerhilfe (Association and Foundation)
- All employees, executives and committee members of partner organisations
- All employees, executives and committee members of social businesses
- All freelancers working for Welthungerhilfe
- All persons and groups volunteering for Welthungerhilfe
- All suppliers and service providers of Welthungerhilfe

The current applicable version of this document is available in the intranet https://bit.ly/2J5QvPH and on the webpage www.welthungerhilfe.org/code-of-conduct

1 Introduction

Digital data processing plays a central role in achieving our business requirements. Almost every process at Welthungerhilfe[1] is supported by or even requires digital solutions. This also includes the processing of and working with private and sensitive data and information of beneficiaries, donors, partners, employees, contractors, suppliers, government agencies and other stakeholders.

The work with and processing of this data and information requires specific protection to prevent unauthorized access, theft, loss, misuse, damage, abuse and/or unjustified change of data and information. It is crucial to Welthungerhilfe to protect this data and information in order to protect the organisation and the people Welthungerhilfe is working with.

This Information Security Policy ("**Policy**") contains general rules in order to ensure Information Security within Welthungerhilfe.

2 Objectives

The objectives of this Policy are to provide a framework for establishing suitable levels of Information Security for all information and data processing systems of Welthungerhilfe and to prevent unauthorized access, theft, loss, misuse, damage, abuse and/or unjustified change of data and information.

Users of data and information at Welthungerhilfe need to understand their responsibilities for protecting the confidentiality and integrity of the data they handle. They need to be aware of and comply with all current and relevant German and EU legislation as well as worldwide standards of information security and protect Welthungerhilfe from liability or damage through the misuse of data and information.

3 Scope

The policy is integral part to the Code of Conduct and applies to:

a) Welthungerhilfe (Association and Foundation) employees, regardless of their type of contract (including full-time employees, temporary personnel, interns and personnel on loan), the scope of their responsibilities and the location of employment.
b) Employees, executives, and committee members of partner organisations[2] receiving material or non-material support from Welthungerhilfe.
c) Employees, executives and committee members of social businesses that Welthungerhilfe holds shares in.
d) Freelancers working for Welthungerhilfe on a contractual basis.
e) People and groups volunteering for Welthungerhilfe (e.g. members of the Programme Advisory Committee or action groups).
f) Suppliers and service providers for Welthungerhilfe.

Members of the Association's bodies (General Assembly, Supervisory Board and Executive Board) of Welthungerhilfe as well as the Foundation's Executive Board and management commit themselves to respecting the policy.

[1] **Welthungerhilfe:** refers to the association Deutsche Welthungerhilfe e.V. and the Stiftung Deutsche Welthungerhilfe.

[2] **Partner organisations:** all local, national, and international partners who have signed a memorandum of understanding or a partnership agreement with Welthungerhilfe, including community-based organisations, civil society groups, non-governmental organisations and advocacy partners.

Hereinafter, the persons specified in points b) through f) above are referred to as Contributors.

This policy is the minimum standard for every individual Employee and Contributor worldwide. It is to be understood in conjunction with the Code of Conduct of Welthungerhilfe and the policies and international standards and codes mentioned therein. In addition, Employees and Contributors must comply with the laws applicable at their place of work. The stricter requirements apply.

Welthungerhilfe cannot be held liable for the actions of Contributors who violate the policy despite prior written consent to the policy.

4 Definition

Information Security is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of data. It is a general term that can be used regardless of the form the data may have (e.g., electronic, physical). Information Security's primary focus is the balanced protection of confidentiality, integrity and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering the organisation's productivity.

Information Security Officer ("ISO") is the responsible person for the development, validation and monitoring of Information Security related processes within the organization's scope of responsibility. The ISO reports the development of Information Security as well as potential and actual violations of Information Security to the Executive Board.

Data Protection Officer ("DPO") is the responsible person for data privacy. The DPO's focus lies on the protection of personal data only.

Information Security Organisation is a team or workgroup working together with the ISO to develop, validate and consult in information security related processes within the organization's scope of responsibility.

5 Information Security Rules

5.1 General Information Security Policy

It is Welthungerhilfe's policy to protect the confidentiality, integrity, and availability of data and information in accordance with applicable legal obligations. This is required to protect the integrity and availability of information technology-based services of Welthungerhilfe. In this regard we implement and review information security measures that ensure alignment and compliance with legislative, policy and operational requirements specific to the work with and processing of data and information. In order to ensure protection of the confidentiality, integrity, and availability of data and information worked with and processed at Welthungerhilfe it is indispensable that everyone working at and with Welthungerhilfe as laid out under 3 above follows and complies with the specific policies laid out in the following:

Data Processing:

Processing of and working with data and information at Welthungerhilfe has to be in compliance with applicable legal obligations and in accordance with the following classification of data adopted by Welthungerhilfe:

a) **Confidential information** includes GDPR[3]-defined special categories of personal data (racial/ethnic origin, political opinion, religious beliefs, trade union membership, physical/mental health condition, sexual life, criminal record), passwords, etc. and should only be accessible to specified members of staff. It should be held in an encrypted modus.

b) **Restricted information** includes GDPR-defined personal data (information that identifies living individuals including home/work address, age, telephone number, photographs), reserved internal draft reports, papers and minutes and should only be accessible to specified members of staff.

c) **Information for internal use only** refers to internal correspondence, final working group papers and minutes, committee papers, etc. and should be only accessible to members of staff.

d) **Public information** is all information that is available on the website of Welthungerhilfe or through Welthungerhilfe's publications scheme and which is made accessible to the public.

Access to and storage of data

- Where sensitive information is stored, processed, or transmitted, access to that information is to be restricted to authorized individuals.
- Areas in which information is stored are to be secured and access restricted to authorized personnel only.
- Work areas are, as far as conveniently possible, to be kept clear of papers and removable storage media containing confidential or restricted information. All Employees involved in the collection, use and disclosure of confidential data and information must sign a non-disclosure and security agreement, if not already covered by an existing contract.
- Contract staff and freelancers not already covered by an existing contract (containing the confidentiality agreement) are required to sign a confidentiality agreement prior to accessing data processed by Welthungerhilfe.

Computer usage policy

As electronic mail is a business resource, one has to note that:

- Personal use of e-mail is to be kept to a minimum.
- The e-mail system is inherently insecure and individuals other than the intended recipients may be able to read messages, therefore no sensitive information classified as confidential information should be sent as part of, or attached to, an e-mail message unless the information is encrypted.
- E-mail attachments are a common source of malicious software and particular care is to be taken before opening any attachments, especially if the message is not from a trusted source.
- Always lock the workstation when leaving the computer, even for a short time.
- Wireless connections (Bluetooth and Wi-Fi) have to be disabled while not needed.
- Antivirus program shall not be disabled. If it is necessary to disable an antivirus program temporarily, the Employee should contact IT.

[3] **GDPR**: the General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA).

- Connections to other networks, including the World Wide Web, are to be protected through a firewall.
- Firewalls must be properly configured to ensure the required level of security is achieved.
- No unauthorized computer software shall be installed or downloaded from the Internet without prior approval of the IT.

Password usage

The following password standards are to be adhered to ensure compliance with the basic principles of Information Security:

- The use of individual passwords is required.
- Sharing of passwords is not permitted.
- Users shall change their passwords if they have any doubt that it has been revealed to someone else.

Data backup

- Information stored on computer systems must be regularly backed-up so that it can be restored if necessary.
- Backup of work-related information and data must be always available on a medium which is directly accessible to Welthungerhilfe.

Virus control policy

User of computers must ensure that the anti-virus software is active on their workstation so that potential viruses from external sources are identified and removed.

Social media policy

- Internet services and social media are to be used responsibly.
- Exchange of work-related information via social media is not permitted.

More information can be found in the following document:

- *Social Media Policy*

6 Reporting Requirements and Consequences for Violations

Anyone with concerns or suspicions about violations of this policy or is aware of incidents must report them immediately. The contact person is the Compliance Unit at the Welthungerhilfe Head Office (complaints@welthungerhilfe.de). Any reports submitted to management or via the national complaint lines of Welthungerhilfe Country offices must be passed on by them to the Compliance Unit. Welthungerhilfe also offers anonymous reporting online or via a telephone hotline for whistle-blowers. All information regarding breaches of this policy is treated as strictly confidential in accordance with the *Organisational Directive on Whistleblowing*. Nobody who reports violations or submits information regarding violations with honest intent, needs to fear any disadvantage or other consequences, even if the report later turns out to be unfounded. It is not the responsibility of Employees and Contributors or whistle-blowers to investigate, provide evidence or decide whether or not breaches of this policy have occurred.

Deliberately false accusations made for the purposes of harming others will not be tolerated. Failure to report incidents also constitutes a violation of the Welthungerhilfe Policies.
Violations of this policy may result in disciplinary action, including termination without notice and/or cancellation of cooperation. Welthungerhilfe will report criminal offences in accordance with the applicable law.

Additional information is provided in the following documents:

- *Complaint Response Mechanism Policy*
- *Organisational Directive Whistleblowing*

Internet: www.welthungerhilfe.org/complaints
Confidential E-Mail-Address: complaints@welthungerhilfe.de
Whistleblowing-Hotline: +49 (0) 228 2288-577

The Policy has been approved by the Executive Board on 10. April 2019.

Mathias Mogge
Secretary General

Christian Monning
Chief Financial Officer