INFORMATION SECURITY POLICY

Genehmigt am:	10.April 2019
Genehmigt durch:	Vorstand
Version:	1
Erstellt durch:	Information Technology
Nächste Überprüfung:	2024
Ansprechpartner*in:	Linda Szelag Leiterin Information Technology Tel.: +49 (0) 228 2288105 IT@welthungerhilfe.de

Bindend für:

- Alle Mitarbeitenden der Welthungerhilfe (Verein und Stiftung)
- Alle Mitarbeitenden, Vorstand und Gremien der Partnerorganisationen
- Alle Mitarbeitenden, Vorstand und Gremien von Social-Business-Unternehmen
- Alle für die Welthungerhilfe freiberuflich arbeitenden Personen
- Alle für die Welthungerhilfe ehrenamtlich tätigen Personen und Gruppen
- Alle Lieferant*innen sowie Dienstleister*innen der Welthungerhilfe

Es gilt die aktuell im Internet (www.welthungerhilfe.de/code-of-conduct) und im Intranet (https://bit.ly/2J5QvPH) verfügbare Version

1. Einleitung

Die digitale Datenverarbeitung spielt eine zentrale Rolle bei der Erfüllung unserer rechtlichen Pflichten. Fast jeder Prozess bei der Welthungerhilfe[1] wird durch digitale Lösungen unterstützt oder erfordert sogar digitale Lösungen. Dazu gehören auch die Verarbeitung von und das Arbeiten mit persönlichen und sensiblen Daten und Informationen von Begünstigten, Geldgeber*innen, Partnerorganisationen, Mitarbeitenden, Auftragnehmenden, Lieferant*innen, Regierungsbehörden und anderen Beteiligten.

Die Arbeit mit diesen und die Verarbeitung dieser Daten und Informationen erfordern einen besonderen Schutz, um Diebstahl, Verlust, fehlerhaften Gebrauch, Beschädigung, Missbrauch und/oder die unberechtigte Änderung von Daten und Informationen oder den unbefugten Zugriff darauf zu verhindern. Für die Welthungerhilfe ist es von entscheidender Bedeutung, diese Daten und Informationen zu schützen, um die Organisation und die Menschen, mit denen die Welthungerhilfe zusammenarbeitet, zu schützen.

Diese Information Security Policy **(„Policy")** beinhaltet allgemeine Vorschriften zur Gewährleistung der Informationssicherheit bei der Welthungerhilfe.

2. Ziele

Die Ziele dieser Policy sind die Schaffung eines Rahmens für die Festlegung geeigneter Informationssicherheitsniveaus für alle Informations- und Datenverarbeitungssysteme der Welthungerhilfe sowie die Verhinderung von Diebstahl, Verlust, fehlerhaftem Gebrauch, Beschädigung, Missbrauch und/oder die unberechtigte Änderung von Daten und Informationen oder den unbefugten Zugriff darauf.

Die Nutzer*innen von Daten und Informationen bei der Welthungerhilfe müssen sich über ihre Verantwortung für den Schutz der Vertraulichkeit und Integrität der von ihnen verwalteten Daten im Klaren sein. Sie müssen alle aktuellen und relevanten deutschen und EU-Gesetze sowie weltweite Standards der Informationssicherheit kennen und einhalten und die Welthungerhilfe vor Haftung oder Schäden durch den Missbrauch von Daten bewahren.

3. Geltungsbereich

Die Policy ist integraler Bestandteil des Code of Conduct und gilt für:

a) Mitarbeitende der Welthungerhilfe (Verein und Stiftung), unabhängig von Vertragsart (u. a. Angestellte, Aushilfen, Praktikant*innen, Leiharbeitskräfte), Umfang und Einsatzort des Beschäftigungsverhältnisses;
b) Mitarbeitende, Vorstand und Gremien der Partnerorganisationen[2], die durch die Welthungerhilfe finanziell oder ideell unterstützt werden;
c) Mitarbeitende, Vorstand und Gremien von Social Business Unternehmen, an denen die Welthungerhilfe beteiligt ist;

[1] **Welthungerhilfe:** bezieht sich auf den Verein Deutsche Welthungerhilfe e.V. und die Stiftung Deutsche Welthungerhilfe.

[2] **Partnerorganisationen:** alle lokalen, nationalen und internationalen Partner, die ein „Memorandum of Understanding" oder ein „Partnership Agreement" mit der Welthungerhilfe unterschrieben haben. Hierzu zählen Community Based Organisations, Civil Society Groups, Non-Governmental Organisations und Advocacy Partner.

d) Freiberuflich arbeitende Personen, die im Rahmen von Werk- oder Honorarverträgen für die Welthungerhilfe tätig sind;
e) Ehrenamtlich tätige Personen und Gruppen (bspw. Mitglieder des Gutachterausschusses, Aktionsgruppen), die für die Welthungerhilfe tätig sind;
f) Lieferant*innen sowie Dienstleister*innen, die für die Welthungerhilfe tätig sind.

Mitglieder der Vereinsorgane (Mitgliederversammlung, Präsidium, Vorstand) der Welthungerhilfe sowie Vorstand und Geschäftsführung der Stiftung Welthungerhilfe bekennen sich selbstverpflichtend zur Achtung dieser Policy. Im Folgenden werden die unter b) bis f) genannten Personen als Mitwirkende bezeichnet.

Diese Policy gilt weltweit als Mindeststandard für jede*n einzelne*n Mitarbeitende*n und Mitwirkende*n. Sie ist im Zusammenhang mit dem Code of Conduct der Welthungerhilfe und den darin genannten Policies sowie internationalen Standards und Kodizes zu verstehen. Zudem haben Mitarbeitende und Mitwirkende die an ihrem Einsatzort geltenden Gesetze einzuhalten. Maßgeblich ist die jeweils strengere Vorgabe.

Die Welthungerhilfe kann nicht für das Handeln von Mitwirkenden haftbar gemacht werden, wenn diese trotz vorheriger schriftlicher Zustimmung zur Policy gegen die Policy verstoßen.

4. Definition

Informationssicherheit bedeutet, unbefugten Zugriff und unbefugte Nutzung, Offenlegung, Beeinträchtigung, Änderung, Untersuchung, Aufzeichnung oder Vernichtung von Daten zu verhindern. Es handelt sich um einen allgemeinen Terminus, der unabhängig von der Form der Daten (z.B. elektronisch, physisch) verwendet werden kann. Der Schwerpunkt der Informationssicherheit liegt auf dem ausgewogenen Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Daten (auch bekannt als die CIA-Triade) bei gleichzeitiger Konzentration auf eine effiziente Umsetzung der Policy, ohne die Produktivität der Organisation zu beeinträchtigen.

Informationssicherheitsbeauftragte („ISB") sind verantwortlich für die Entwicklung, Validierung und das Monitoring von informationssicherheitsrelevanten Prozessen, die im Verantwortungsbereich der Organisation liegen. Sie berichten dem Vorstand über die Entwicklung der Informationssicherheit sowie über mögliche und tatsächliche Verletzungen der Informationssicherheit.

Datenschutzbeauftragte („DSB") sind verantwortlich für den Datenschutz. Der Tätigkeitsschwerpunkt von Datenschutzbeauftragten liegt ausschließlich auf dem Schutz personenbezogener Daten.

Die **Informationssicherheitsorganisation** ist ein Team oder eine Arbeitsgruppe, das oder die mit ISB zusammenarbeitet, um informationssicherheitsrelevante Prozesse, die im Verantwortungsbereich der Organisation liegen, zu entwickeln und zu überprüfen sowie diesbezüglich zu beraten.

5. Vorschriften zur Informationssicherheit

5.1 Allgemeine Information Security Policy

Die Policy der Welthungerhilfe besteht darin, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen in Übereinstimmung mit den geltenden gesetzlichen Verpflichtungen zu schützen. Dies ist erforderlich, um die Integrität und Verfügbarkeit von informationstechnisch basierten Diensten der Welthungerhilfe zu gewährleisten. Diesbezüglich vollziehen und überprüfen wir Informationssicherheitsmaßnahmen, welche die Angleichung an die sowie die Einhaltung von gesetzlichen, operativen und Policy-Anforderungen sicherstellen, die für die Arbeit mit und die Verarbeitung von Daten und Informationen kennzeichnend sind. Um Vertraulichkeit, Richtigkeit

und Verfügbarkeit von Daten und Informationen zu gewährleisten, die bei der Welthungerhilfe verarbeitet und verwendet werden, ist es unerlässlich, dass alle, die bei und mit der Welthungerhilfe wie in Abschnitt 3 beschrieben arbeiten, die nachfolgend dargelegten spezifischen Policies befolgen und einhalten:

Datenverarbeitung

Die Verarbeitung von und das Arbeiten mit Daten und Informationen bei der Welthungerhilfe müssen den geltenden gesetzlichen Verpflichtungen und der folgenden, von der Welthungerhilfe übernommenen Klassifizierung von Daten entsprechen:

a) **Vertrauliche Daten:** Dazu gehören die in der Datenschutz-Grundverordnung[3] definierten speziellen Kategorien personenbezogener Daten (rassische/ethnische Herkunft, politische Meinung, religiöse Überzeugung, Gewerkschaftszugehörigkeit, körperlicher/seelischer Gesundheitszustand, Sexualleben, Strafregister), Passwörter usw. Diese Daten dürfen nur bestimmten Mitarbeitenden zugänglich sein. Vertrauliche Daten müssen verschlüsselt gespeichert werden.

b) **Eingeschränkte Daten:** Dazu gehören personenbezogene Daten gemäß DSGVO (Daten, mit denen lebende Personen identifiziert werden können, einschließlich Haus-/Arbeitsadresse, Alter, Telefonnummer, Fotos), zurückgehaltene, interne Berichtsentwürfe, Dokumente und Protokolle, auf die nur bestimmte Mitarbeitende Zugriff haben dürfen.

c) **Informationen, die ausschließlich für den internen Gebrauch bestimmt sind:** Dazu gehören interne Korrespondenz, abschließende Arbeitsgruppenpapiere und -protokolle, Gremienpapiere usw. Diese dürfen nur für Mitarbeitende zugänglich sein.

d) **Öffentliche Informationen** sind alle Informationen, die auf der Website oder über das Publikationssystem der Welthungerhilfe verfügbar sind und so der Öffentlichkeit zugänglich gemacht werden.

Zugriff auf und Speicherung von Daten

- Werden sensible Daten gespeichert, verarbeitet oder übertragen, so ist der Zugang zu diesen Daten auf autorisierte Personen zu beschränken.
- Bereiche, in denen Daten gespeichert werden, sind zu sichern und dürfen nur autorisiertem Personal zugänglich sein.
- An Arbeitsplätzen sollten sich keine Dokumente und Wechselmedien mit vertraulichen oder eingeschränkten Daten befinden, soweit dies arbeitsorganisatorisch sinnvoll möglich ist. Alle Mitarbeitenden, die an der Erfassung, Nutzung und Offenlegung vertraulicher Daten und Informationen beteiligt sind, müssen eine Verschwiegenheits- und Sicherheitserklärung unterzeichnen, sofern sie dazu nicht bereits durch einen bestehenden Vertrag verpflichtet sind.
- Mitarbeitende und freiberuflich Tätige sind verpflichtet, vor dem Zugriff auf die von der Welthungerhilfe verarbeiteten Daten eine Verschwiegenheitserklärung zu unterzeichnen, sofern sie dazu nicht bereits durch einen bestehenden Vertrag (der eine Verschwiegenheitserklärung enthält) verpflichtet sind.

[3] **DSGVO:** Die Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) ist eine Verordnung im EU-Recht über Datenschutz und Privatsphäre für alle Personen, die in der Europäischen Union (EU) und dem Europäischen Wirtschaftsraum (EWR) leben.

Policy zur Computernutzung

Da das E-Mail-System eine Organisationsressource darstellt, ist Folgendes zu beachten:

- Die persönliche Nutzung des E-Mail-Systems ist auf ein Minimum zu beschränken.
- Das E-Mail-System ist prinzipiell unsicher, sodass andere Personen als die vorgesehenen Empfänger*innen E-Mail-Nachrichten lesen können. Daher dürfen keine sensiblen Daten, die als vertraulich eingestuft sind, als Teil einer E-Mail-Nachricht oder als Anhang einer E-Mail-Nachricht gesendet werden, es sei denn, die Daten sind verschlüsselt.
- E-Mail-Anhänge sind eine häufige Quelle für bösartige Software, weswegen vor dem Öffnen von Anhängen besondere Vorsicht geboten ist, insbesondere wenn die Nachricht nicht von einer vertrauenswürdigen Quelle stammt.
- Sperren Sie den Bildschirm jedes Mal, wenn Sie den Arbeitsplatz – selbst für kurze Zeit – verlassen.
- Drahtlose Verbindungen (Bluetooth und WLAN) müssen deaktiviert werden, wenn sie nicht benötigt werden.
- Das Antivirenprogramm darf nicht deaktiviert werden. Wenn es notwendig ist, ein Antivirenprogramm vorübergehend zu deaktivieren, ist die IT-Abteilung zu kontaktieren.
- Verbindungen zu anderen Netzwerken, einschließlich des World Wide Web, müssen durch eine Firewall geschützt werden.
- Firewalls müssen ordnungsgemäß konfiguriert sein, um sicherzustellen, dass der erforderliche Sicherheitsgrad erreicht wird.
- Ohne vorherige Zustimmung der IT-Abteilung darf keine unautorisierte Computersoftware aus dem Internet installiert oder heruntergeladen werden.

Umgang mit Passwörtern

Die folgenden Passwortstandards sind zu befolgen, um den Grundprinzipien der Informationssicherheit zu entsprechen:

- Die Verwendung von individuellen Passwörtern ist erforderlich.
- Die Weitergabe von Passwörtern ist nicht erlaubt.
- Die Nutzenden sind verpflichtet, ihre Passwörter zu ändern, wenn sie nicht ausschließen können, dass sie anderen Personen offengelegt wurden.

Datensicherung

- Auf Computersystemen gespeicherte Informationen müssen regelmäßig gesichert werden, damit sie bei Bedarf wiederhergestellt werden können.
- Gesicherte arbeitsbezogene Informationen und Daten müssen stets auf einem für die Welthungerhilfe direkt zugänglichen Medium verfügbar sein.

Antiviren-Policy

Nutzende von Computern müssen sicherstellen, dass die Antivirensoftware auf ihrem Computer aktiv ist, sodass potenzielle Viren aus externen Quellen identifiziert und entfernt werden.

Social Media Policy

- Internetdienste und Social Media sind verantwortungsbewusst zu nutzen.
- Der Austausch von arbeitsbezogenen Informationen über Social Media ist nicht erlaubt.

Nähere Informationen liefert das folgende Dokument:

- Social Media Policy

6. Meldepflicht und Konsequenzen bei Verstößen

Wer Vorfälle, Bedenken oder Verdachtsmomente in Bezug auf Verstöße gegen diese Policy hegt bzw. von Vorfällen weiß, ist verpflichtet, diese unverzüglich zu melden. Ansprechpartner ist hierfür die Compliance-Abteilung in der Welthungerhilfe-Zentrale (complaints@welthungerhilfe.de). Hinweise, die an Vorgesetzte oder über die nationalen Beschwerdestellen der Welthungerhilfe erfolgen, müssen von diesen an die Compliance-Abteilung gemeldet werden. Darüber hinaus ermöglicht die Welthungerhilfe eine anonyme Meldung im Internet oder telefonisch über die Whistleblowing-Hotline. Alle Informationen über Verstöße gegen diese Policy werden in Übereinstimmung mit der *Betriebsvereinbarung Revisionstatbestände (Whistleblowing)* streng vertraulich behandelt. Niemand, der in redlicher Absicht Verstöße meldet oder Hinweise auf Verstöße gibt, muss Nachteile oder sonstige Konsequenzen befürchten, auch dann nicht, wenn sich die Meldung oder der Hinweis später als unbegründet herausstellt. Es liegt nicht in der Verantwortung von Mitarbeitenden und Mitwirkende bzw. Hinweisgebenden, Untersuchungen anzustellen, Beweise zu liefern oder zu entscheiden, ob Verstöße gegen diese Policy vorliegen oder nicht.

Bewusst falsche Anschuldigungen, die den Zweck verfolgen, anderen zu schaden, werden nicht geduldet. Auch die Nichtmelden von Vorfällen stellt eine Verletzung der Welthungerhilfe Policies dar.

Verstöße gegen diese Policy können disziplinarische Maßnahmen bis hin zur fristlosen Kündigung und/oder die Annullierung der Zusammenarbeit zur Folge haben. Straftatbestände bringt die Welthungerhilfe unter Beachtung des jeweils geltenden Rechts zur Anzeige. Nähere Informationen liefern die folgenden Dokumente:

- *Betriebsvereinbarung Revisionstatbestände (Whistleblowing)*
- *Complaints Response Mechanism Policy*

Internet: www.welthungerhilfe.de/beschwerde
Vertrauliche E-Mail-Adresse: complaints@welthungerhilfe.de
Whistleblowing-hotline: +49 (0) 228 2288 577

Die Policy wurde vom Vorstand am 10. April 2019 genehmigt.

Mathias Mogge
Generalsekretär

Christian Monning
Finanzvorstand