Evidence Action

Global Information Management Policy

1. PURPOSE AND APPLICATION 2
2. POLICY 2
2.1 Principles of Information Management 3
Roles of Content Owner and Content Manager 3
Ownership 4
Information Management Environment 4
Working with Third-Parties 5
Waiver Procedure 5
Annual Review 5
2.2 Information Creation & Collection 6
2.3 Information Classification 6
Information Classifications 6
2.4 Information Storage & Security 9
Staff Working Folders 10
Information Security Breach Notification 11
2.5 Information Access and Sharing 11
Access 11
Sharing 11
Information Retrieval 12
2.6 Information Retention & Destruction 12
Retention 12
Destruction 12
Suspension of Record Disposal In Event of Litigation or Claims 13
3. Collection and Handling of Personal Data 13
Principles of Data Collection: Personal Data 13
Principles of Data Collection: Consent 13
Principles of Data Collection: Rights of the Data Subject 14
Principles of Data Collection: Notices to the Data Subject 14
Data Protection Impact Assessments 14
4. DEFINITIONS 14

5. COMPLIANCE AND REPORTING 16
6. APPENDICES.....17
Appendix A - Guidance for On/Offboarding 17
Appendix B - Annual Review Checklist.....17
Appendix C - Information Retention Schedule 17
Appendix D - Country-Specific Regulatory Considerations.....17
Appendix E - Data Protection Impact Assessment.....17

Information Management Policy	Policy Effective Date: February 1, 2023
	Policy Owner: Global Operations
	Policy Number: GO.GL

1. PURPOSE AND APPLICATION

This Information Management Policy (IM Policy) provides the policy and procedures regarding the Evidence Action information management environment, including the use, storage, management, sharing, security, and access to company documents, data, and other electronic records. The purpose of this policy is to safeguard all company information and data and to support the ongoing operations of Evidence Action.

This policy applies to all Evidence Action employees.

Use of Evidence Action systems constitutes consent to these guidelines and an understanding that possible disciplinary action may occur if misuse or abuse of these systems is discovered.

2. POLICY

Background

Evidence Action makes use of a variety of data to create information relating to its operations and programs. Evidence Action collects and stores information of many types in a variety of formats. The relative importance and sensitivity of this information varies and is subject to Evidence Action's Information Classification procedure.

In collecting and using this information, Evidence Action is subject to legislation, regulations, and funder/partner rules controlling how this information can be handled and the safeguards that must be put in place to protect it. Evidence Action also believes in the inherent value of safeguarding information and therefore abides by additional best practice even when not legally or contractually required to do so.

Sensitive organizational information must be protected from loss of integrity, confidentiality, or availability. The risks of inadequate access controls range from inconvenience to critical loss or corruption of information. It is important that Evidence Action information is – as far as it can be protected from loss, destruction, falsification, unauthorized access, and unauthorized release. A range of controls are used to ensure information security including backups, identify management, and encryption.

2.1 Principles of Information Management

There are a number of key principles that must be adopted when creating a compliant information management environment. These principles apply regardless of format or medium.

All information will be:

- Collected for a specified, explicit, and legitimate purpose;
- Relevant and limited to what is necessary;
- Accurate and remain up to date (except where older/archive information is necessary for historical purposes);
- Classified according to the Evidence Action Information Classification procedure;
- Retained in a form which allows identification for disposition;
- Stored and shared in compliance with all applicable legal, regulatory, and contractual requirements;
- Shared only with approved/authorized parties;
- Secure during the entire life-cycle; and
- Destroyed in accordance with an approved schedule.

All users will be aware of good information management practices and will receive training as required for their position. If in doubt, staff should consult Global Operations.

Roles of Content Owner and Content Manager

Content Owner and Content Managers serve in key roles as designated custodians for managing a group of information and ensuring compliance with this policy.

Content Owners (CO) are ultimately responsible for ensuring teams' compliance with the IM Policy and empowering their Content Manager(s) to effectively implement the IM Policy. Content Owners make the final decision on information access, classification, and use. They are *not* usually involved with the day to day administration of the IM Policy within their team.

- Approve authorized users access to folders and files with confidential information. Remain aware of information sharing and access permissions and work closely with the Content Manager to maintain compliance with the IM Policy.
- Understand where confidential information is in their team's folder structure.

- Approve access to Confidential information for internal users and access to all External party access.
- Resolve issues that the Content Manager escalates to them.
- Approve or reject, in consultation with GO, any Waiver Requests for the IM Policy. In most cases, the IM Policy will be flexible and a waiver may not be necessary.

Content Managers (CM) administer information management policies and guidelines for a designated group of information. They are the point person on their team for understanding and implementing the Information Management policy. A team may have more than one Content Manager.

- Ensure access to and sharing of their team's information in compliance with information classifications
- The CM should consult with the CO before granting access to:
    - A third party external to Evidence Action
    - Any confidential information owned by the team
- Administer information lifecycle - including organization, categorization, access, storage, and removal/archival for information generated by their team
- Conduct Annual Review in consultation with GO to ensure compliance with both in-country regulations and the IM policy
- Understand waterfall and sharing permissions on Box
- Ensure implementation of IM Policy requirements
- Support on/offboarding of staff within their team (see Appendix A for guidance on On/offboarding)

Ownership

'Ownership' refers to the department/team that is *responsible* for a set of information - including managing user access, maintaining the folder structure, and reviewing information flagged for disposal. Any piece of information should be owned by one department/team (i.e. teams should not maintain duplicate copies of the same information). Content Owner is the designated decision maker and person responsible for a set of information 'owned' by a department/team.

Information Management Environment

Information stored, received, accessed, or sent over Evidence Action's information systems is not in the personal/private domain; rather, it is ultimately owned by Evidence Action, and may be accessed at any time. Deletion of any electronic information may not truly eliminate the information from the system. Information that is stored or transmitted through Evidence Action systems is not the property of the user, and Evidence Action maintains rights to the access and possession of this information.

Evidence Action reserves the right to directly access information stored on a system or device owned by the organization, or require users to reveal passwords to Evidence Action as necessary.

Working with Third-Parties

Evidence Action will ensure that all transactions it enters into with individuals or entities outside of Evidence Action which involve the sharing of information will contain specific terms regarding information management. These terms should draw from the principles identified above, essentially extending the same governing principles to the work of partners. Terms should make specific reference to activities to be undertaken, resources to be used, and clearly allocating lines of responsibility. The Director of Grants and Contracts should be consulted in all cases. If there is a conflict between this Policy and the requirements of a specific funder, the funder's requirements will take precedence and the deviations will be documented in writing. If so, the Content Manager must follow the Waiver Policy.

If there is a conflict between this Policy and the requirements of a third-party (for example, data collection firms, universities, government ministries), Global Operations will conduct an analysis and determine whether any deviation will be made from this Policy. All deviations will be documented in writing. If so, the Content Manager must follow the Waiver Policy.

Waiver Procedure

The purpose of the Waiver Policy is to ensure that all deviations from the Information Management Policy are approved and documented. To request a deviation from the Information Management Policy, a written request must be sent to Global Operations for approval with the Content Owner on copy via email.

1. The sections of the Information Management Policy being deviated from;
2. The reason for deviation;
3. The anticipated length for which the deviation will last;
4. The anticipated impact, if any, from deviation. This may include, but is not limited to, exposure of sensitive information, exposure of Evidence Action systems, exposure of personal proprietary data without consent;
5. Any necessary remediation that must be undertaken during deviation, or once the deviation is complete;

Acknowledgement and approval via email from Global Operations and the Content Owner(s), approving deviation from the Information Management Policy. Depending on the severity of the exception, additional leadership may need to be formally included and their approval acquired. Any additional approvers will be requested by Global Operations. Once a waiver is completed and approved, the employee must save a copy of the waiver and approval in Box.

Annual Review

Annually, each Content Manager will conduct a review to ensure that all information for their department is created, stored, accessed, and destroyed appropriately.

Global Operations will work with Content Managers to determine when the review will take place. Global Operations will help Content Managers complete the review for their area of responsibility, using the Annual Review Checklist in Appendix B as a guide. The review reports shall be documented, stored within the Global Operations' files and shared with Content Owners.

2.2 Information Creation & Collection

Employees at Evidence Action should use approved applications when creating, composing, and editing documents and information. Global IT maintains a list of approved applications; for more information, please contact Global IT.

Box is Evidence Action's designated primary file storage system. As such, it is preferred that staff use Box to both create and store information. If you are storing personally identifiable information (PII) or sensitive information, it MUST be stored in Box.

Use Box:

- For storage of all final versions of documents
- To create a single, coherent location for organizing related-documents (i.e. project files, even if they contain bookmarks to other storage locations)
- To bookmark key files stored in other locations/systems (i.e. Google Drive)
- When creating and storing Confidential information (MANDATORY)
- For collaborating or sharing information with external parties

Use Google Drive

- For collaboration on and drafting of non-confidential documents

When collecting data and information, employees should use company-approved data collection and analysis tools as required by employee responsibilities. These may include, but are not limited to, the following: R, ODK, Stata, ArcGIS, etc.

2.3 Information Classification

All information can be classified according to the below stated Classification Schema which is used to guide Access Control. This policy applies to information in all formats or media. Information assets are classified according to the risks associated with information being stored or processed. Information with the highest risk needs the greatest level of protection to prevent compromise; information with lower risk requires proportionately less protection. Three levels of classification will be used to classify information based on how the information is used, its sensitivity to unauthorized disclosure, and requirements imposed upon its care of use.

The purpose of these information classification categories is to guide employees' routine interaction with Evidence Action information. These guidelines apply to all types of information Evidence Action uses globally. If there are questions regarding the proper handling and use of information, an employee should direct questions to Global Operations.

Information Classifications

Company information can generally be categorized in three ways; employees should assess the information they interact with and handle it in accordance with the respective security control guidelines.

I. Public

Information explicitly or implicitly approved for distribution to the public without restriction. It can be freely distributed without potential harm to Evidence Action, donors, affiliates, or individuals. Public information generally has a very low sensitivity since by definition there is no such thing as unauthorized disclosure, but it still

warrants protection since the integrity of the information can be important. Examples include Evidence Action's website, employee directories, press releases, etc.

II. Internal

Information intended for internal business use only with access restricted to a specific workgroup, department, group of individuals, or affiliates with a legitimate need. Internal information is generally not made available to parties outside of Evidence Action. Unauthorized disclosure could adversely impact the company, donors, affiliates, or individuals. Internal data generally have a low to moderate sensitivity. Examples include: financial accounting data not containing confidential information; company intranet; programmatic data that doesn't contain PII; company strategic plans; HR, IT, or other company policy documents.

III. Confidential

Highly sensitive information intended for limited, specific use by a workgroup, department, or group of individuals with a legitimate need-to-know. Explicit authorization from the Content Owner is required for access because of legal, contractual, privacy, or other constraints. Unauthorized disclosure or transfer of information could have a serious adverse impact on the core business functions of the company or its affiliates, the personal privacy of individuals, or on compliance with federal, state, or foreign laws and regulations. Confidential information has a very high level of sensitivity. Examples include: Social Security numbers, credit card data, personally identifiable information including individual donor records, passport numbers, medical records, authentication data, passwords etc. Information and data may also be sensitive if protected under a confidentiality clause in a contract with a partner or donor. All PII, personal, or sensitive data MUST be classified and stored in a Confidential folder that is labeled as such.

If the classification is not known or unsure, employees should treat all material as confidential until the classification is confirmed.

The following table defines required safeguards for protecting information based on classification.

Security Control Category	Information Classification		
	Public	Internal	Confidential
Access Controls	- No restriction on viewing. - Authorization by owner required for modification.	- Viewing and modification might be restricted to authorized individuals as needed for business-related roles. - Content Owner permission required for access, plus approval from supervisor. - Authentication and authorization required for access	- Viewing and modification restricted to authorized individuals as needed for business-related roles. - Content Owner permission required for access, plus approval from supervisor. - Authentication and authorization required for access. - Confidentiality agreement may be required.
Copying and Printing	- No restrictions	- Information should only be printed when there is a legitimate need.	- Information should only be printed when there is a legitimate need.

		- Information should be limited to individuals with a need to know. - Information should not be left unattended on the printer. - Folders should be labeled “Internal”.	- Information must be limited to individuals authorized to access the information. - Information should not be left unattended on a printer. - Files should be labeled “Confidential”.
Network Security	- May reside on a public network.	- Protection with a firewall is recommended. - Information should be stored in a folder with restricted permission settings on the company’s file system (Box).	- Protection with a firewall is recommended. - Information should be stored in a folder with maximum restricted permission settings on the company’s file system (Box).
System Security	- Must follow general best practices for system management and security. - Computer antivirus & firewall recommended.	- Must follow company’s policies and practices for system security and computer management. - Computer antivirus & firewall required.	- Must follow company’s policies and practices for system security and computer management. - Computer antivirus & firewall required.
Physical Security	- System should be locked or logged out when left unattended.	- System required to be locked or logged out when left unattended. - Not to be viewed in public or common areas.	- System required to be locked or logged out when left unattended. - Not to be viewed in public or common areas. - Physical access to offices, computers, devices, and storage media must be controlled and limited to authorized employees only at all times.
Data Storage	- Storage on a company provided cloud storage location recommended.	- Must be stored in an authorized, company provided cloud storage location. - Should not be solely stored on an individual’s workstation or mobile device. If temporarily downloaded to an individual’s workstation or mobile device, should be deleted as soon as no longer needed. - Should only be maintained on approved systems/applications.	- Must be stored in an authorized, company provided cloud storage location. - Should not be stored on an individual’s workstation or mobile device. If temporarily downloaded to an individual’s workstation or mobile device, should be deleted as soon as no longer needed. - Paper or hard copies should not be left unattended, and should be stored in a secure location.

Transmission	- No restrictions	- When transmitting, it is strongly encouraged to utilize a secure Box or Google Drive link. - Make all attempts to limit the distribution of information to those within Evidence Action or authorized outside parties.	- Encryption or password required - Cannot be transmitted via email attachment; should be transmitted via secure Box or Google Drive link. - Make all attempts to limit the distribution of information to only authorized individuals. - Confidentiality agreement may be required.
Disposition (NOTE: No electronic hardware will be disposed of prior to IT reviewing the items and properly sanitizing)	- Regular trash disposal for physical information. - Normal delete and overwrite for electronic information.	- Shredding or burning for physical information. - Delete, overwrite, degaussing/ demagnetizing for electronic information. - If electronic sanitization is not possible, shredding, crushing, or incineration are options.	- Shredding or burning for physical information. - Delete, overwrite, degaussing/ demagnetizing for electronic information. - If electronic sanitization is not possible, shredding, crushing, or incineration are options.

2.4 Information Storage & Security

Evidence Action's designated primary file storage system is Box. All files and other electronic documents related to Evidence Action business are to be stored in the appropriate location within Box. In limited cases, if a file cannot be stored on Box, a bookmark should be put in Box to direct users to the file location (i.e. Google Drive).

A key advantage of Box is visibility and long-term continuity. Because Box is centrally managed and owned, files are more easily found by employees. When an employee departs Evidence Action, their files remain in Box for future discoverability.

Evidence Action's secondary file collaboration system is Google Drive. Google Drive may be used for documents that are actively being edited, reviewed, and collaborated upon. All final versions of documents in Google Drive should be stored in Box for long-term retention; draft or active documents should be bookmarked in Box for easier accessibility.

Accounts for other cloud-based storage systems (such as Dropbox, OneDrive) are not supported, and any Evidence Action-related files should not be stored on these non-authorized systems.

If necessary to ensure compliance with in-country regulations, a separate or additional local storage system may be adopted with approval from Global Operations to store sensitive information (e.g. raw data with personal identifiers, etc.).

In all cases, file storage must meet the following requirements:

1. Country-level storage: If country data regulations apply to the information, then information should be held in a structure allowing for country-specific controls. (i.e. PII to be held in in-country servers or in country-specific Box folders)
2. Least Permission Possible: Staff should have the least permission level possible to perform their duties, only content authorized for company-wide sharing should be accessible to all staff.
3. Classification: All Confidential folders should be clearly marked as much. All folders without an explicit classification shall be classified as Internal by default. Evidence Action-Administered Systems: Content should only be stored on Evidence Action Administered systems (i.e. Box, Google Drive, etc.)
4. Designated Ownership and Management: Information will have at least one designated Content Owner and one designated Content Manager.

The master copy of all Evidence Action files must be stored in Box. It is a violation of Evidence Action policy to store Evidence Action files on individual devices - whether the device is owned by the Company or the individual - without the master copy stored in Box. It is permissible for employees to temporarily store files Locally on their device. Should an employee's device become compromised due to a crash, virus, loss or theft the employee understands that those files could be lost.

Employees are prohibited from permanently storing Evidence Action files on personal devices or any other non-approved service. Please see the Global IT Policy (IT.GL.06) for more information on use of personal devices. Where information is legally (or practically) required to be stored on paper or another non-electronic medium (eg: photographs, textile, etc.), adequate precautions must be taken to ensure that environmental conditions remain suitable for the type of material used. Where possible, digital backup copies of such information should be made by scanning or photographing the items. If the original paper copies are not needed and the digital record is sufficient, the original paper copy should be destroyed. Regular checks must be made to assess the rate of deterioration of the material and action taken to preserve the items as required in accordance with the Information Retention and Destruction Policy (section 2.6).

Staff Working Folders

At the time of onboarding, a 'staff working folder' shall be set up for each individual by Box Admin. This folder is where staff should store their draft and working documents. All final and key documents should be stored within the appropriate departmental folder in Box.

New Countries or Programs

When Evidence Action adds a new program or initiates operations in a new country:

- a corresponding folder structure should be set up in Box to securely maintain information relating to all programs and country operations
- The structure of the folder should be Country Folder > Department Folder
    - Within each Department folder, all PII or sensitive information should be held in a folder that is clearly labeled "Confidential"
- Department folders should be standardized to match the current structure in the same department across locations i the same region

- a Content Owner shall be designated for the Country folder
- a Content Owner and Content Manager shall be designated for each Department folder

Information Security
Where appropriate to the classification level and the storage medium, additional security will be used to ensure the confidentiality and integrity of the information. Such additional security may include encryption or password protection for electronic information or storage in locked cabinets, closed offices, or at secure off-site storage facilities for physical information.

Care will be taken to ensure that information is stored securely for the life of the object and in compliance with the Global IT Policy (IT.GL.05 and IT.GL.07).

Information Security Breach Notification

Where a Breach of information security is known or believed to have occurred, the user(s) will *immediately* notify the IT department and the Content Owner. Wherever possible, the notification shall include:

- name and contact information of the person reporting the breach;
- nature of the breach;
- details of the types of personal information compromised, if any;
- number of departments affected by the breach;
- number of individuals' whose personal information has been affected by the breach;
- cause of the breach;
- date and timeframe of the breach, if known;

2.5 Information Access and Sharing

Access to Evidence Action's information will be secured in order to prevent breach of confidentiality, integrity, or availability.

Access

Users will only access Evidence Action's systems using their assigned credentials. Using another user's credentials to access systems is not permitted. All Evidence Action information classified as "Internal" or "Confidential" will not be released outside of the approved user pool except for authorized business purposes. Authorized business purposes are determined by Content Owners (or if designated, Content Managers). If in doubt, staff should consult Global Operations.

Sharing

External sharing and collaboration of data with third-parties must be approved by the Content Owner. In some cases, consulting with the Director of Grants and Contracts is advised. (see "Working with Third Parties" above) Personal use of such assets or performing unauthorized work for another employer or institution is not permitted. Under no circumstances are employees to use Evidence Action materials, equipment and/or property for personal or personal political ends.

Evidence Action information classified as “Internal” or “Confidential” will not be transmitted using personal email, unauthorized file storage accounts (such as Dropbox or similar), personal chat channels (such as WhatsApp or similar), or other personal devices (such as flash drives, hard drives, or similar).

Information Retrieval

Information must be stored in a retrievable and usable format. This might require retaining particular hardware or software so the information can be accessed. For archival information, a balance must be struck between the cost of storage and the speed of retrieval so that the most likely business and compliance needs can be met.

2.6 Information Retention & Destruction

Content Managers are responsible for overseeing implementation of the Information Retention and Destruction Policy in their respective departments and functions. If clarification or guidance is needed, they should consult with Global Operations.

Retention

Company information and records shall be adequately maintained until they are no longer needed by the organization or are of no value. The Information Retention Schedule, in Appendix C, defines how long information must be retained. At least one copy of each document/record will be retained according to the schedule.

This applies to all physical and electronic records generated in the course of Evidence Action’s operation, including both original documents and reproductions/copies. Electronic documents include e-mail, web files, text files, sound and movie files, PDF documents, and all Microsoft Office or other formatted files.

The Information Retention Schedule which applies in all circumstances unless a funder stipulates otherwise. Where there is a conflict between the Information Retention Schedule and the requirements of a funder, Evidence Action follows the requirements of the funding source.

Destruction

Once information has reached the end of its life according to the appropriate Information Retention Schedule, it must be securely destroyed in a manner that ensures that it can no longer be used.

Hard copies of documents will be destroyed by shredding or fire after they have been retained until the end of the period stated in the Information Retention Schedule. Electronic information and information stored in cloud systems will be destroyed by deleting the records per the cloud systems’ official instruction. Hardcopies of computer backups will be destroyed by fire or other proven means to destroy such media after they have been retained until the end of the Information Retention Schedule.

When relying on a third-party to destroy information (eg: cloud service providers, off-site information storage facilities, etc.), information destruction processes must be reviewed, documented, and approved by Global Operations prior to contract execution.

Suspension of Record Disposal In Event of Litigation or Claims

If any litigation, claim, or audit is started before the expiration of the stated retention period, the records shall be retained until all litigation, claims, or audit findings have been resolved and final action taken.

If any employee becomes aware of an investigation or audit concerning Evidence Action or the commencement of any litigation against or concerning Evidence Action that affects the retention schedule, such employee shall inform the Content Owner. The Content Owner shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of information.

3. Collection and Handling of Personal Data

Collection and handling of Personal Data comes with additional regulatory requirements. This section provides guidance on Evidence Action's standards for data collection and processing of an individual's Personal Data. This guidance is based on a review of the various data protection regulations in the countries where Evidence Action operates (at the time of writing). Adherence to these guidelines will, in most cases, ensure compliance to local laws.

In some particular cases, additional country-specific considerations need to be taken into account to ensure compliance. See Appendix D - Country-Specific Regulatory Considerations

Principles of Data Collection: Personal Data

In collection, processing, storing, or using the personal data of another person, the following principles shall guide our processes.

1. Privacy and Accountability: Data shall be processed in accordance with the right to privacy of the data subject and remain accountable to them.
2. Unambiguous Consent: Data subject must provide unambiguous consent in advance of data collection and processing.
3. Fair and Lawful: Have legitimate grounds for collecting data and not use it in any way that may have unjustified adverse effects on the individual
4. Relevant and Necessary: Only collect/process/store/use data that is relevant to the purpose and not excessive or unnecessary data.
5. Accuracy and Quality: Ensure accuracy and quality of information that is collected/processed/stored/used and where necessary, kept up to date. Reasonable measures shall be taken to rectify or erase inaccurate data.
6. Retention: Information shall be retained only for the period authorized.
7. Transparency: Provide information about the data processing when requested by the data subject.
8. Secure: Observe security safeguards with respect to data.

Principles of Data Collection: Consent

1. Collection and processing of personal data requires consent.
2. Consent must be 'unambiguous', in advance of data collection, and recorded. The data subject (or parent/guardian) must understand the questions being asked of them, how the information will be used, and can make a choice about if and how to respond.

3. If collecting personal data from a minor/child (any person under the age of 18), consent is required from parent/guardian.

Principles of Data Collection: Rights of the Data Subject

The individuals from whom we collect their personal data have the following rights:

1. Informed of Use: Be informed of the use to which their personal data is to be put.
2. Correction: Correction of false or misleading data.
3. Deletion: Deletion of false or misleading data about them.
4. Access and Portability: Access their personal data in custody of a data controller or data processor and transmit their data to another data controller/processor.
5. Objection to Consent: Object to the processing of their personal data.

Principles of Data Collection: Notices to the Data Subject

Before collecting data from an individual, the individual needs to be informed (in a language and manner that they can understand) of the following:

1. The nature and category of data being collected.
2. Contact information for the person/institution collecting the data.
3. Purpose for data being collected.
4. Whether providing data is discretionary or mandatory.
5. Consequences of failure to provide data (i.e. none).
6. If providing data is legally required.
7. Who will be recipients of data.
8. That person's right to access, correct, delete the data.
9. The right to prevent/object to processing of data.
10. The period for which the data will be retained.
11. The intention to transfer data to another country or processor.

Data Protection Impact Assessments

Data Protection Impact Assessments (DPIA), see Appendix E, are to be completed by Content Managers and submitted to the Content Owner and to Global Operations any time a new data collection process is to be implemented or there is a significant change in an existing data handling process (including, for example, a change in the data collection/handling technology). DPIAs also apply to the collection and handling of data in prospective and/or new countries. A DPIA is designed to consider if appropriate privacy protections are in place and determine whether a new data collection process is compliant.

4. DEFINITIONS

Access - the ability to make use of information (See also Permissions).

Archive - to place information into long-term storage; a location or media used for long-term storage.

Business Process - a sequence of linked tasks and related decisions that result or contribute to the delivery of a good or service.

Breach or Compromise - unauthorized access to systems or disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional access to, disclosure, modification, destruction, or loss of information may have occurred.

Compliance - acting in accordance with an agreed upon standard or criteria. This can refer to performance measurements, laws, or partner regulations.

Content Owner - the individual solely responsible for changes to access permissions. They are ultimately responsible for content including: access, classification, use. Examples: country, department, program leads

Content Manager - the individual designated by Content Owner who ensures adherence to information management policies and guidelines for a designated group of information, Considered the administrator of information lifecycle - including organization, categorization, access, storage, and removal/archive. The person who escalates issues to the Content Owner.

Data - objects that, when combined, create information. Data is a subset of information.

Data Subject - an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored.

Encryption - the translation of information into a form that is unintelligible without a deciphering mechanism.

Essential information - information that is needed to meet operational responsibilities and to protect the legal and financial rights of the organization.

Guideline - recommended guidance that provides further information on, and/or interpretation of the associated policy, SOP, or Business Process.

Information - processed, structured, and organized data.

Information Classification or Classification - categorizing information against a matrix containing six elements: three elements measuring impact and three elements measuring access.

Information life cycle - the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Information management - the collection and handling of information, both electronic and physical, from one or more sources and the distribution of that information to one or more audiences. Information management includes the development and implementation of policies, processes, procedures, and tools.

Information sharing - the distribution of information to authorized users to support internal or external programs or partners.

Information security - protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Official record - any information, regardless of physical form, that is required to be retained for a specific period of time due to legal, regulatory, or contractual obligations. Official records document decisions or actions taken by the organization relating to internal or programmatic matters.

Permissions - allowable user actions (e.g. create, read, write, destroy).

Personal Data - information about a person from which the person can be identified, that is recorded in any form and includes data that relates to- (a) the nationality, age or marital status of the person; (b) the educational level, or occupation of the person; (c) an identification number, symbol or other particulars assigned to a person; (d) identity data; or (e) other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual.

Personally identifiable information or PII - information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual; For example, SSN, National ID number, DOB, Employee dependent information, personal address, banking information, W-4, W-2, W-9, 1099, 401K or other pension information, passport, driver's license. Other examples include criminal, medical, legal, and financial records, login credentials, and passwords.

Policy - mandatory written rules which must be followed as applicable;

Standard Operation Procedure or SOP - a detailed written description of a Business Process that aims to ensure consistency and quality in process execution;

Storage - the location where information is filed and retrieved during the information life cycle. Storage can be electronic or physical;

Tool - templates, forms, charts, informational and any other material prescribed for use in conjunction with an element of Policy, Guideline, Business Process, or SOP;

Training - teaching people the knowledge and skills that will enable them to perform their jobs more effectively;

User - a person or entity with authorized access.

5. COMPLIANCE AND REPORTING

Any person to whom this Policy is applicable is expected to report known or suspected contraventions of this policy following the procedures set forth in Whistleblower Policy within the Code of Conduct (HR.GL.01).

6. APPENDICES

Appendix A - Guidance for On/Offboarding

ONBOARDING

The Hiring Manager should work with the departmental Content Manager to assign the appropriate level of access to folders.

Content Owner/Manager Roles

Will the person joining serve in a Content Owner or Content Manager role?

- If yes, please notify Global Operations so they can provide the appropriate training materials.

OFFBOARDING

Content Owner/Manager Roles

Does the person leaving serve in a Content Owner or Content Manager role?

- If yes, please notify Global Operations who will re-assign the Content Owner or Content Manager role

Staff Working Folder on Box

If the employee has files/information in their 'staff working folder' in Box, incorporate moving those files into the appropriate departmental folders into the offboarding plan.

Google Drive

- Ensure that ownership of key files and folders is transferred to other team members.
- Consider consolidating files into folders and transferring ownership of those folders, so information doesn't get 'lost.'
- Consider creating a file map of key files and folders for other team members to reference.

Appendix B - Annual Review Checklist

Template HERE

Appendix C - Information Retention Schedule

HERE

Appendix D - Country-Specific Regulatory Considerations

Country Regulatory Review Summary Decks

Appendix E - Data Protection Impact Assessment

Step 1: Identify the need for the Assessment

Explain broadly what the project aims to achieve and what type of data collection and processing it involves. It may be helpful to refer or link to other documents.

Step 2: Describe the Processing
1. Describe how you plan to collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone in other countries or outside of Evidence Action?
2. Describe the nature of the data, is the data PII or sensitive/high risk? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?
3. Describe the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of data collection/processing? 4. Describe the purposes of the data collection/processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for Evidence Action, and more broadly?

Step 3: Consultation process
Who else do you need to consult or involve within the organization to make them aware? Do you need to consult with a third-party partner (i.e. government ministry, research partner)?

Step 4: Assess necessity and proportionality
Describe the steps you will take to ensure compliance to country data protection regulations. Is the data collection and processing process you've designed legal and compliant?Does your designed process achieve your desired outcome; is there another way to achieve that outcome? How will you ensure data quality? What information will you give individuals and how will you help to support their rights? What measures do you take to ensure data collectors and data processors follow your process? How will you safeguard any international transfers (and have you reviewed local regulatory requirements for transfer)?

Step 5: Identify and assess risks
Describe sources of risk, likelihood of that risk occurring, and the severity of impact on individuals. Include associated risk to compliance and corporate risks as necessary.

Step 6: Identify measures to reduce risk
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk.

Prepared by (Dept Rep):
In consultation with (MLE-D Rep):
Approved by (GO and CO):

*Review by country-level DPO, if applicable.