BILL & MELINDA GATES foundation

The Bill & Melinda Gates Foundation Written Information Security Program

Version September 2021

Contents

Objective

The Bill & Melinda Gates Foundation ("foundation") is a nonprofit organization fighting poverty, disease, and inequity around the world. The objective of the development and implementation of this comprehensive written information security program ("WISP"), is to document the administrative, technical, and physical safeguards for the protection of Sensitive Information in place at the foundation and affiliated entities. The WISP sets forth our procedure for evaluating and addressing our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Sensitive Information.

Purpose

The purpose of this document is to summarize the security controls the foundation and affiliate entities have in place to protect Sensitive Information. The foundation follows industry best practices and regularly evaluates its information security program to make adjustments to protect against new and emerging threats.

For purposes of this document, "Sensitive Information" means Confidential Information, Personal Data, and other information that the Foundation labels or indicates should be treated as sensitive. "Confidential Information" whether written, oral, or observed, means: (a) information relating to foundation's directors, officers, strategies, finances, investments, grants, contracts, program related investments, facilities, events, guests, or security; (b) employee and third-party information (including personal information) that the foundation must treat as confidential or private; and (c) any other information that the Foundation labels or indicates should be treated as confidential or which, under the circumstances of disclosure, ought to be treated as confidential. "Personal Data" means any data that relates to an identified or identifiable natural person.

Scope

This document details the information security program and controls in place to safeguard Sensitive Information under the custodianship of the foundation and affiliated entities. For data hosted at third-party service providers, the foundation relies on the security controls put in place at those organizations. The foundation negotiates contract terms to include, wherever possible, specific security terms which would address minimum security controls required at a service provider. Required controls for third-party service providers must at least meet those required at the foundation. For additional information about how the foundation manages third party service provider relationships and risk, see the section below titled "Third Party Service Providers".

Information Security Governance

Information Security for the foundation is provided by a dedicated team of information security professionals, who are part of the Global Security team, whose responsibilities reach to all foundation locations and affiliated entities across the globe. Information Security focuses on protecting foundation data. The Information Security Director has been appointed as Security Officer. The Information Security Director reports to the Chief Security Officer who oversees all aspects of the security program.

The foundation has a Code of Conduct Policy and Digital Information Security Policy, both endorsed by the Executive Leadership Team. These policies lay out the responsibilities of the foundation staff to comply with applicable laws and regulations and to follow foundation provided information security requirements. Adherence to these policies is a condition of employment.

Policies prohibit inappropriate use of electronic tools and technologies. Foundation employees utilizing the foundation network and computing assets are required to conduct themselves in a manner consistent with organizational policies regarding confidentiality, business ethics, use of technology and professional standards. Those who violate the Digital Information Security Policy are subject to disciplinary action, up to and including dismissal.

People connecting to the foundation network are required by policy to conduct themselves in a manner consistent with guidelines regarding confidentiality, business ethics, use of technology and professional standards. The organization requires that communications via these connections comply with applicable US laws and regulations, including restrictions on the use of telecommunications technology and encryption in foreign countries and copyrights and license agreement terms and conditions.

Human Resources Security

Background Checks

Newly hired personnel undergo pre-employment background checks. Depending on the level of hire, these checks may include (note that the type of checks performed may be limited by jurisdiction and local laws):

- Social Security number trace
- Education verification
- Criminal convictions are searched for seven years (federal, state, county and national)
- Department of Motor Vehicle license information
- Professional licenses/certification
- Employment history verification
- National Sex Offender Registry check

Security Awareness Training

Security awareness communications and trainings are managed by a multi-disciplinary group of professionals from Information Security, Physical Security and Legal. Staff receive ongoing communications and trainings to reinforce security awareness around technology, physical security, privacy, confidentiality and ethics and compliance responsibilities.

Termination and Change of Employment

Account access to foundation systems and to those operated on behalf of foundation are promptly disabled upon separation or termination of the user, or when access is longer required. Deprovisioning notices are automated in the enterprise resource planning system.

Access Control

The foundation follows a formal process to grant or revoke access to foundation resources. System access is based on the concepts of least-privilege and need-to-know-access, to ensure that authorized access is commensurate with defined responsibilities. Depending on the application, the organization uses a combination of user-based, role-based and rule-based access control approaches.

Wherever technically feasible, the foundation uses strong, industry standard authentication methods. Additionally, foundation staff is required to use Multi-Factor Authentication (MFA) to access foundation resources (including remote access).

The foundation has established documented procedures for secure creation and deletion of user accounts, including processes to disable and/or delete accounts for terminated personnel. All workforce members are required to agree to take precautions to protect the integrity and confidentiality of security credentials.

Access to servers and other IT infrastructure in an admin, root or system level capacity is limited to the appropriate administration staff. This access is reviewed and approved by IT management.

The Identity and Access Management Standard establishes password requirements that include password change, reuse, and complexity. Inactivity timeouts are enforced after 15 to 30 minutes, depending on the sensitivity of the application accessed. Accounts are locked after no more than six (6) failed authentication attempts in less than 30 minutes and may be automatically unlocked after 30 minutes of lockout.

Physical Security

Foundation data is hosted both on-premises and in multiple cloud environments. On-site access to the foundation data center requires a key card and access is restricted to authorized individuals only. All hosted (cloud) environments are SOC audited and ISO 27001 compliant. In general, data centers use a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources.

Security systems and supporting controls are implemented in foundation offices to provide access control, video monitoring of building perimeters and passageways, and auditing services. The systems are supported with alarm devices and a 24/7/365 monitoring service with response protocols.

The foundation has a policy to support the types of access privileges assigned to authorized individuals. The organization's HR system sends out notices to the Security Team allowing for timely management of staffing transactions. Administrators also manage access privileges based on roles and responsibilities. Foundation staff are required to carry and display an access badge with credentials to allow individuals to be identified as authorized individuals.

Operations Management

The foundation's Global Technology Services organization has established and maintains standard operating procedures, governance process, including a repository of procedures, formal review and approval processes, and revision management.

Device Security Controls

All laptops are protected with disk-level encryption. The software enforces password controls. Training is delivered to new staff, to educate them about physical security risks and to encourage behavior that will help protect laptops against theft and are part of annual security acknowledgements.

Foundation issued mobile devices are centrally managed and configured with security policies which enforce device encryption, passwords, a limited number of login attempts before locking, and the ability to remote wipe the device and data.

The foundation uses enterprise class security solutions to provide a secure computing environment. These solutions are centrally managed and configured to automatically retrieve updates.

Laptops run a security suite, which includes antivirus, anti-malware, endpoint detection and response (EDR), firewalls, and whole disk encryption.

Data Backups

Data stored on premises is backed up daily, encrypted and stored securely in redundant locations. The foundation utilizes cloud-based back up services and geo-redundancy for data hosted in the cloud.

Data Transfers

Only approved, secure protocols are allowed for transfers of Sensitive Information within the foundation and between the foundation and third parties.

Data Encryption

Information classified as "Sensitive Information" is encrypted at rest using industry standard algorithms. Sensitive Information hosted at third party service provider organizations is required to be encrypted per contract terms.

Data Deletion and Asset Disposal

At least annually, employees are required to delete or destroy data and records that are no longer useful and not historically significant. In addition, employees are required to delete, destroy, or anonymize any personal data once it is no longer needed to fulfill the purpose(s) for which it was collected or as otherwise required or permitted by applicable laws or agreements.

Foundation assets are destroyed using US Department of Defense (DoD) standards once they no longer have business value per our Asset Management Standard. Assets are only retained past their useful life to satisfy regulatory or legal requirements. Computing systems containing data (hard drives, etc.) are erased using DoD industry standards before being recycled or disposed.

Logging and Monitoring

System audit logs from production systems are collected and stored for analysis and review. Logs are protected from tampering as they are sent to a central, secure repository. As some cloud vendors do not allow direct access to logs, access may be given when permitted by the vendor for investigative purposes.

Security logs from production systems are configured to alert the security operations center when a security related event is detected. All alerts are reviewed by qualified cybersecurity analysts and responded to as the situation warrants.

Vulnerability Scanning

The foundation has established processes and procedures for performing periodic assessments of IT systems. External penetration tests are performed annually by a qualified third party. Results are remediated as needed.

The foundation maintains a private network using industry best practices to ensure the security of sensitive and personal information. This network is regularly assessed through third party vulnerability and penetration testing.

Third Party Service Providers

The foundation requires that providers be aware of and contractually bound to adhere to information security requirements and restrictions. Standard third-party agreements include security control requirements. These requirements include and are not limited to: a documented information security policy, protection of information assets, physical protection controls, return or destruction of information, non-disclosure, security awareness training, change management, access control policy including the use of unique IDs, access authorization process, reporting and investigation of security breaches, right to monitor access, annual review of security requirements, escalation process and applicability to additional subcontractors.

Select vendors considered as “high risk” (access to sensitive information or physical access to foundation offices) are assessed as part of the foundation’s third-party risk management program. The third-party risk management program requires vendors to complete questionnaires and provide third-party audits or attestation reports. The foundation performs on-site risk assessments at vendors as it deems necessary.

Information Security Incident Management

Foundation staff are required by policy to report known or suspected security incidents. A dedicated email is available to team members for reporting security incidents to the Security Group. Security staffs are on call 24/7/365 to immediately address security related activities.

The foundation has documented procedures for staff and third parties receiving reports of security incidents. The foundation has documented incident response processes, which include pre-defined roles and responsibilities, and an automated call process for escalations and communications. Procedures for legal

review and notification of impacted individuals are built into the process. Once an incident has closed, a root cause analysis is performed and mitigations to prevent future incidents are put in place.

The incident response process is tested regularly and revised as needed.