BILL & MELINDA GATES foundation

Digital Information Security Policy

1.0 Purpose

Each of us is responsible for keeping the foundation's digital information and information systems secure from intentional or accidental harm. The purpose of this policy is to outline the steps you must take to protect our digital information and information systems.

2.0 Scope

This policy applies to any individual or entity (*e.g.*, employee, contingent worker, vendor, grantee, partner) who has access to the foundation's digital information or information systems.

3.0 Policy

The foundation's digital information systems include any application, device, laptop, hardware, or software that interacts with foundation digital information, including cloud-based and third-party hosted systems. You are required to take the following measures to keep these systems secure:

3.1 Report suspected security issues.

Immediately report to the IT Service Desk any circumstance where a device containing foundation information has been lost, stolen, hacked, seized through legal action, or otherwise security-compromised. Report any circumstance where you suspect your foundation account credentials may have been compromised.

3.2 Protect your passwords.

Keep passwords secure. Passwords may not be shared with anyone at any time for any reason except when required by law.

3.3 Obtain a security risk assessment on all new technologies.

Submit all new technologies and digital systems (*e.g.*, messaging tools, online storage tools, mobile applications) to the foundation's Information Security department for a security risk assessment prior to implementation for foundation business.

3.4 Do not use tools that could be harmful.

Do not use tools that are designed to assess security or to attack computer systems or networks, including password crackers, vulnerability scanners, and network sniffers without specific authorization from the foundation's Information Security department. Do not run programs, software, processes or automated transaction-based commands that are intended to disrupt or could reasonably be expected to disrupt, damage or degrade foundation computers or network usage, including performance, software and hardware.

3.5 Stay abreast of information security risks.

Participate fully in required information security training.

3.6 Only share sensitive information with authorized individuals on a need-to-know basis.
Before sharing sensitive information, determine whether the recipients are authorized to receive such information. This includes all members of e-mail distribution lists, and recipients of instant messages, documents, or other communications.

4.0 Responsibilities

Global Security is responsible for implementing and enforcing this policy. Exceptions may only be reviewed and granted by the CBOO.

Your compliance with this policy is a condition of your work with the foundation. Non-compliance may result in termination of your relationship with the foundation. If you have any questions regarding this policy, please contact: InfoSec@gatesfoundation.org.

5.0 Procedures, Standards, Guidelines and Other Related Documents

Code of Conduct
Records Management Policy
Information Classification Standard
Online Social Media and Communications Policy
Privacy Policy

6.0 Revision History

Effective Date	*Approved By*	*Modification*
08/22/2016	Todd Pierce, CDO	New document replacing Technology Usage Policy
05/01/2017	Connie Collingsworth, CBOO	Added sections 5.1 (d) and (f)
07/30/2019	Connie Collingsworth, CBOO	Removed mobile device requirements, added enforcement and exception roles to 5.0