UNFPA
Policies and Procedures Manual
Security Policy

ICT SECURITY POLICY

<table>
<thead>
<tr>
<th>Version number</th>
<th>Review date</th>
<th>Reviewed by</th>
<th>Approval date</th>
<th>Approved by</th>
<th>Summary of Changes</th>
<th>Next review date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Jul 2012</td>
<td>G. Price</td>
<td>Jul 2012</td>
<td>J. Ilag</td>
<td>Baseline</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>Dec 2015</td>
<td>G. Price</td>
<td>Jan 2016</td>
<td>J. Ilag</td>
<td>Updated list of prohibited sites in para 5; added para 6 to emphasize staff responsibility</td>
<td>Jul 2017</td>
</tr>
</tbody>
</table>

A. Policy objective:

1. The most important issue that arises when talking about computer security is the security of data. In compliance with organizational mandates and generally accepted industry best practices, UNFPA provides for the security and privacy of the data stored on, redirected through, or processed by its technology resources. Throughout this policy, the term “user” identifies full and part-time staff members, consultants, temporaries, interns, retirees, vendors and other users affiliated with third parties who access organizational company technology resources due to their job responsibilities. Management expects users to comply with this and other applicable policies, procedures, and laws.

B. Intended audience:

2. Effective information security requires user involvement as it relates to their jobs. Users are accountable for their actions and therefore they own any events occurring under their user names. It is the user’s responsibility to abide by policies and procedures of all networks and systems with which they communicate. Information and Communications Technology (ICT) staff has a critical role as they are responsible for security infrastructure, policy enforcement, and prevention of security breaches. Details of ICT staff responsibilities can be found in the Security Policy for ICT Staff.

C. Policy statement:

a. Ownership:

3. UNFPA encourages the use of its technical resources; however they remain organizational property and are offered on a privilege basis only.

b. Monitoring:

4. UNFPA reserves the right to monitor, review and log user use of its technology resources without notice. This includes but is not limited to email, Internet access, file access, log-ins and changes to access levels. Furthermore, and consistent with generally accepted business practices, UNFPA collects statistical data about its technology resources and ICT staff monitors its use to ensure the ongoing availability and reliability of systems. Should a security
or other relevant incident arise, UNFPA may review system logs to determine the cause and take appropriate action.

c. **Staff Responsibilities and Accountability:**

5. Access of personal or private Internet Service Providers while using UNFPA provided information technology resources or using non-company provided information technology resources to conduct company business do not indemnify any entity from the responsibilities and compliance with this policy. It is important to remember that electronically transmitted information travels through many networks, and many different computer connections, thus compromising security. User responsibilities include but are not limited to:

- **Access and release only data for which you have authorized privileges and a need to know.**
- **Sensitive information should not be stored on external storage systems (e.g. Dropbox, unencrypted USB memory sticks and external hard drives) or similar devices.** Even with protective measures in place, data saved on such systems is vulnerable. If the use of external storage is an operational necessity, the proper sensitivity classification must be specified, approval obtained from the head of the unit, and the storage should be utilized for data transfer only – with immediate deletion following completion of the transfer.
- **Cloud storage should only be used for UNFPA data if there exists an official agreement or contract between UNFPA and the third party service (e.g. Google Drive).** The problem with individual users engaging these third parties to house their data is that there are no contractual controls as to who has access to the data or any knowledge of the due diligence used by the third party service in protecting the data. Thus, users could be inadvertently revealing sensitive data to unauthorized persons.
- **The Internet may not be used for illegal purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, harassment, intimidation, forgery, impersonation, gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).**
- **Individuals must limit their personal use of the Internet.** UNFPA allows limited personal use for communication with family and friends, independent learning, and public service, but prohibits, inter alia, use for mass unsolicited mailings, access for non-users to UNFPA resources or network facilities, uploading and downloading of files for personal use, access to pornographic sites, peer to peer sites, illegal drugs, weapons, gaming, competitive commercial activity, and the dissemination of chain letters.
- **Users remotely accessing UNFPA’s corporate network should ensure that their remote access connection is given the same consideration as the user's on-site connection (e.g. an updated antivirus system is running).**
- **Abide by and be aware of all policies and laws applicable to computer system use.**

6. It is the responsibility of all staff to report IT security violations to the ICT Officer or designee and cooperate fully with all investigations regarding the abuse or misuse of UNFPA IT resources. If it is determined that a security incident arose, in whole or in part, due to user noncompliance with applicable regulations, rules, policies or procedures, this may result in forfeiture of the privilege to use technology resources as well as administrative, disciplinary or other legal action as applicable.
7. Protect user IDs and maintain password confidentiality.

8. Passwords are the primary means of providing user access to system resources. Once a particular resource is compromised, other systems can be compromised as well, resulting in the possibility of disclosure of organizational and personal information. To prevent information theft, users must ensure the confidentiality of all passwords used to connect to UNFPA systems. Users must follow the password guidelines listed below:
   - Do not write your password down or disclose it via e-mail.
   - Do not give your password to anyone.
   - If your password has been disclosed, change it immediately.

9. User passwords should be changed periodically. The current policy is to require password changes every 90 days.

10. When creating a new password, the guidelines are:
    - Length Minimum: 8 characters
    - There will be a password history of three, meaning that the same password cannot be used when asked to change.
    - Default passwords must be changed immediately.
    - Use mixtures of numbers, special characters, capital letters, and small letters (should simpler passwords be used, then 12 characters is recommended).
    - Should be easy to remember.
    - Should not be so obvious that someone can guess it.

11. Log off systems or initiate a password protected screensaver before leaving a computer unattended.

12. Use only UNFPA acquired and licensed software.

D. Policy date:

13. The Security Policy was issued on 18 July 2012 (originally approved and issued on 18 July 2012 with subsequent revisions as shown in the beginning of this document) will remain in force without time limit, and will be reviewed annually to ensure relevance.

E. Policy owner:

14. The MIS Chief is responsible for ensuring IT security.

F. Change authority:

15. The MIS Chief, Technology Services Section Chief, and Infrastructure/Security Specialist have the authority to change the security policy. The Director of DHR can give exception
waivers. Exception waivers should be logged and reported to the ICT Board on a quarterly basis.