Fighting Hunger Worldwide

WFP World Food Programme
wfp.org

Executive Director's Circular

(Information Technology Division)

Date: 5 May 2015
Circular no.: OED2015/012
Revises:
Amends:
Supersedes: EDD2011/004

WFP Corporate Information and IT Security Policy

1. WFP relies on its global information technology (IT) systems and the integrity and availability of information processed, delivered and stored therein.

2. The purpose of this Circular is to announce the updated WFP Corporate Information and IT Security Policy (attached). This is the framework policy document for all activities related to the access to and use of all WFP IT systems.

3. This document describes the policies and relevant roles and responsibilities for:

   a) accessing and using all IT systems and the Internet;
   b) constructing and protecting passwords;
   c) managing security threats (such as viruses);
   d) protecting IT equipment and information; and
   e) handling confidential information protected by copyright and licensing agreements.

4. The measures described apply to all WFP staff members and to anyone granted access to any WFP electronic information system. Routine compliance audits will be conducted to ensure that these guidelines are adhered to.

5. WFP Corporate Information and IT Security Policy comes into effect immediately.

Ertharin Cousin
Executive Director

Fighting Hunger Worldwide

WFP
World Food Programme
wfp.org

Information Technology

Corporate Information and IT Security Policy

Table of Contents

1. Introduction

a. Information security is the ongoing process of exercising due care and diligence to protect information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

b. WFP information systems and networks are an integral part of the Organization[1] and are fundamental to its continued success. Substantial human resources and financial investments go into maintaining them and ensuring that they continue to evolve in order to meet the changing requirements of the Organization, both at HQ and in the field.

c. Inadequate information security and continuity is a substantial business risk that threatens not only important organizational assets, but also business processes critical to the continued operations of the Organization. Information security is therefore of enormous significance to WFP, calling for a security structure that is sophisticated enough to balance the conflicting demands of protecting WFP corporate information and information infrastructure, and the privacy of WFP system users.

2. Scope

a. This Circular applies to all WFP personnel, including but not limited to international professional staff members, general service staff members, locally recruited staff members, UN volunteers, individuals recruited on Special Service Agreements (SSA), Service Contracts (SC), consultants, interns, TAUs, and volunteers. All individuals cited above, will be referred to as "personnel" in the context of this policy. Parts of this policy may also apply to third parties with whom special arrangements have been made.

b. This policy applies to all information systems owned by and/or operated by WFP. It is intended to support the protection, control and management of the Organization's information assets which includes data and information[2] that is:

- stored in databases, on computers or in the Cloud;
- transmitted across internal and public networks; and
- stored on removable media, e.g. CD-ROMs, hard drives and pen drives.

3. Objective

a. WFP information is maintained on the principles of integrity, confidentiality, availability and accountability. This information should be available when required, accessible by authorized personnel, and trusted to be authentic while maintaining assigned confidentiality.

[1] In the context of this document, "Organization" refers to WFP.
[2] Section 3.1 of ST/SGB/2007/5 ('All records, including electronic records and e-mail records, created or received by a staff member in connection with or as a result of the official work of the United Nations, are the property of the United Nations').

b. This policy has been established in order to:

- enable secure access to needed services for the user community;
- protect the significant resource investment that the Organization has put into its information systems and networks;
- protect information contained within these systems from unauthorized access;
- ensure the continuity of IT systems usage;
- guarantee the privacy and accuracy of information resources;
- detect and prevent IT security threats, violations and security incidents;
- reduce business and legal risks;
- contribute to the protection of the name and reputation of the Organization;
- minimize the risk of information loss, data corruption, data access disruption, and unauthorized information disclosure; and
- comply with internal regulations and rules.

4. Administration

a. The IT Security Office in HQ, under the Chief Information Officer (CIO) and headed by the IT Security Officer is responsible for the administration of this policy.

b. Requests for exceptions to this policy should be addressed to the IT Security Officer via the IT Service Desk.

5. Classification of Information

a. To ensure appropriate and sound handling of corporate information, its classification according to the dimensions of confidentiality, availability, integrity and accountability shall be applied.

- Confidentiality means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. The classification levels are:

✓ Strictly Confidential	Information of highly sensitive nature requiring that access be limited to the recipient(s) designated by the information owner and requiring particular safeguard measures to prevent theft and unauthorized access.
✓ Confidential	Information of sensitive nature, to be restricted to recipients determined by the information owner. Examples of “confidential” documents: Audit Reports, Personnel Records, Accounting and Payroll Records, correspondence marked “Confidential”.

✓ Internal	Information of non-sensitive nature, for internal use in WFP only, open to information sharing and available for free circulation within WFP. Examples of "official use only" document types: Legal agreements, invoices, orders, project documents, etc.
✓ Internal UN	Information of non-sensitive nature open to information sharing and available for free circulation within the UN system.
✓ Public	Information of non-sensitive nature accessible to the public. The "work of the United Nations should be open and transparent", consequently classifying information as public should be considered generously. Examples of public records: disclosed Governing Body Documents, Press Releases, Annual Reports, Publications, etc.

- Availability means ensuring timely and reliable access to and use of information. The classification levels are:

✓ Always	The information must always be available and accessible to authorized consumers. That is likely an on-line system.
✓ Business hours	The information is accessible to authorized consumers during normal business hours. It may not be accessible on weekends for example.
✓ On request	The information may not be always available immediately. This is for example the case for archived records or documents requiring research.

- Integrity in this policy means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. The classification levels are:

✓ Required	The information must be precise, reliable and verifiable.
✓ Desirable	The information should reflect the truth but may include uncertain elements.
✓ Loose	The information is indicative and cannot be used as reference.

b. The information owner applies the classifications to the information assets she/he is accountable for.

c. Where portions of information can be classified independently (e.g. some fields in a record are more confidential than others) different classifications are applied to the

single subsets. The overall classification of the entire information asset will always reflect the most restrictive value amongst the information subsets.

d. The information classification determined by the information owners should be recorded in an appropriate system[3]. Other actors should be given the ability to view the information classification and treat the information according to the rules implied by the classification.

Metadata

e. Along with the classification of the information assets, metadata (information about the data) is an important contribution to its successful management. The metadata collection for each information asset should include:

- a brief description;
- references to the systems processing it;
- indications on quality and value to the Organization; and
- relationships with other information assets.

f. All information resources must be handled in compliance with this policy and the Programme's internal regulations, including Directive AD2006/006, "Directive on Records Retention Policy in WFP" and Directive CP 2010/001, "WFP Directive on Information Disclosure".

6. Statement of responsibility

a. Information security is every personnel's responsibility, while using WFP IT systems, WFP personnel are expected to conduct themselves in accordance with the ICSC Standards of Conduct for The International Civil Service[4]. By logging onto any WFP IT system users affirm that they have read, understood and acknowledged this policy and agree to abide by the WFP Code of Conduct[5].

b. Roles and general responsibilities pertaining to this policy as a whole are set forth in this section and are performed by the following categories of individuals:

- IT Security Officer;
- IT personnel;
- Information Owner;
- Information Custodian;
- Information User;
- Supervisor; and
- Personnel.

c. Any additional, specific responsibilities assigned to each of the roles are stated in the relevant policy sections to which they apply.

[3] Refer to Annex B
[4] http://icsc.un.org/resources/pdfs/general/standardsE.pdf
[5] WFP Code of Conduct; http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp268899.pdf

d. The Chief Information Officer (CIO) is ultimately responsible for the effective achievement of the objectives set out in this policy document.

IT Security Officer responsibilities

e. In addition to monitoring usage of IT systems against this policy, the IT Security Officer advises and recommends on all security matters and releases regular IT Security advisories designed to increase IT security awareness.

f. The IT Security Officer:

- assesses the information and network security framework and recommends enhancements to the CIO as appropriate;
- develops, maintains and implements standards and procedures necessary to enhance and maintain information security within the Organization;
- periodically probes the network and information systems for vulnerabilities and responds appropriately;
- leads efforts to respond promptly to security incidents;
- oversees the implementation of and compliance with this policy, including systems to assist in the monitoring and management of compliance;
- provides appropriate support and guidance to assist personnel and supervisors fulfil their responsibilities under this policy; and
- regularly prepares security status and compliance reports for the CIO, including reports of potential deviations and violations to this policy.

IT personnel responsibilities

g. IT supports the management and operational objectives of WFP by assuming responsibility for the technology infrastructure, systems development and information management. IT personnel play a vital role in connecting WFP offices and partners, providing access to the Organisation's information resources.

h. IT personnel shall:

- install and maintain up-to-date end-point protection software on all WFP computers and mobile devices;
- have up-to-date security patches on servers, PCs, laptops and mobile devices;
- be responsible for responding to virus attacks, attempt to destroy any virus detected, and document each incident;
- monitor compliance with this policy and report apparent violations as stated in paragraph 17 (h);
- shall abide by the WFP Privacy and Data Protection Principles set out in this document policy; and
- regularly inform personnel/users about newly released IT guidelines and policies, expected code of conduct and responsibilities.

Information Owner Responsibilities

i. Information Owners are units or responsible persons who have some authority over the information. They may generate the information, they may have approval rights over the information, they may be data owners of a Master Data domain[6] or possess other forms of control rights over the information[7].

j. Information owners must:

- authorize access to owned information based on established rules and criteria;
- classify information in accordance with Directive AD2006/006, "Directive on Records Retention Policy in WFP" the definitions set out in point 5 (Information Classification) of this policy;
- define any additional controls required to further protect information; and
- review information usage reports on usage patterns so Information Owners can ensure only those authorized are accessing information.

Information Custodian Responsibilities

k. Information custodians have physical or logical possession of WFP information or information that has been entrusted to WFP. Custodians are IT personnel, or personnel assigned IT responsibilities and/or system administrators.

l. Information custodians:

- operate and maintain information systems infrastructure on behalf of information owners and users;
- configure owner and user requirements within the information systems so as to best preserve their accessibility, confidentiality and permissions;
- configure access permissions as requested by the information owners and enable access traceability;
- keep a detailed log of system changes; and
- provide reports, upon request, to information owners about information system operations and availability.

Information User Responsibilities

m. Information users are WFP personnel who use or access information that is owned or under the custody of WFP or others. They are authorized to use WFP computers, information and network systems and features. Information users are responsible for

[6] WFP Master Data Governance Framework
http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp264965.pdf

[7] Directive AD2006/006 on Records Retention Policy identifies owners as "Responsible Units" and the information for which they own is defined in Annex B, 'File Plan and Retention Schedules': http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp090363.pdf. The Director of the Division or Chief of the Branch indicated are considered the information owners.

observing the security policies, standards and rules established by the information owners.

n. Information users shall:

- protect basic WFP interests by preventing unauthorized disclosure of records according to the classification of documents defined in this policy and in Directives AD2006/006, "Directive on Records Retention Policy in WFP" and CP 2010/001, "WFP Directive on Information Disclosure";
- observe the confidentiality classifications as set in point 5 (Information Classification);
- familiarize themselves with and adhere to the provisions of this policy;
- report malfunctions and other incidents which may suggest that an information system may not be functioning well;
- report suspicious activity to local IT Officers in Country Offices and the IT Service Desk in HQ;
- protect their credentials, i.e. the login user name and password, and not disclose them to anyone else;
- not misrepresent, obscure, suppress or replace their own or other personnel's identity on the Internet or on any other WFP information system;
- not leverage their access to information and information systems in order to misrepresent themselves and/or WFP to external parties; and
- use WFP resources responsibly.

Supervisor Responsibilities

o. Supervisors:

- ensure that all personnel within their supervision are aware of and comply with this policy; and
- share notifications of apparent non-compliance confidentially with the CIO.

Personnel Responsibilities

p. Personnel shall:

- where WFP has provided appropriate solutions, make sure records classified as Strictly Confidential and Confidential are encrypted[8] when stored on portable media devices;
- seek supervisory permission when copying strictly confidential and confidential information to a portable drive, unless the information is related to the personnle's own record;
- never store strictly confidential and confidential information on private and/or non-WFP authorized equipment, environments and/or services (see Annex B for the authorized options);

[8] Refer to WFP encryption guidelines provided in Annex C of this policy.

- take caution of their surroundings when viewing information while away from WFP premises;
- exercise extra caution when printing, copying or faxing strictly confidential and confidential information to prevent the information from being revealed to unauthorized parties; and
- ensure that printers, copiers or fax machines are not left unattended following jams or malfunctions while printing, photocopying or transmitting strictly confidential and confidential information.

7. **LAN and Information Systems Access and Use Policy**

a. A computer network covering a small, physical area is referred to as a Local Area Network (LAN). The WFP LAN provides access to WFP information systems. Access to the LAN and WFP information and information systems is provided based on business need and the personnel's role within the Organization.

b. Information systems include WFP applications and third party software containing WFP information.

c. Personnel are identified in a system, network or application by a unique name usually referred to as a *User ID*, *User name*, or *E-mail Address*. For access to the LAN, personnel must obtain the appropriate credentials (i.e. a User ID and password combination). Personnel are authenticated (i.e. granted access) to a system through a User ID and password combination.

d. All systems are configured to monitor and log system access. Event details are stored and periodically reviewed.

e. When an individual's role or job responsibilities change or when they leave the Organization, access must be appropriately updated or removed.

f. Access to core information systems such as the WFP Information Network and Global System (WINGS), WFP's resource management system, is not permitted for personnel who separate from WFP. Access to other IT systems may be granted on an exceptional basis for a period of up to three months. Requests for continued access should be made by managers to the IT Service Desk and shall be considered on a case by case basis by IT Security in consultation with the CIO.

g. All systems are managed by at least one administrator who has been granted access privileges above those of a standard user for the exclusive purpose of ensuring maximum availability, integrity and security of the systems for which they are responsible.

h. The additional access privileges held by administrators mean that during the course of their activities, they may need to access information which is held by, or concerns, other users. Such information must neither be acted upon, nor disclosed to any other person unless required as part of a specific investigation.

i. Access control measures for system administrators are to be particularly robust to reflect the privileged access they will have to WFP information systems and detailed audit log functionality must be enabled on all systems.

j. Non-WFP equipment[9] must not be connected to the WFP LAN without prior authorization from the IT Security Office in HQ via the IT Service Desk, and in the field from the relevant field IT officer, IT assistant or IT focal point, whoever is more senior. Any equipment connecting to the WFP LAN must meet the following minimum security requirements:

- device is registered with the Active Directory Domain global.wfp.org;
- latest security and operating system (e.g. Windows 7 or higher) patches are installed;
- anti-virus software is up to date;
- have no unlicensed or prohibited software installed; and
- mobile devices (smart phones and tablets) must be registered on the WFP corporate Mobile Device Management portal[10].

k. Non-WFP or non-compliant equipment may be connected to WFP wireless networks which have been specifically created for this use. Information on such networks is available from the IT Service Desk at HQ and the IT Officer in country offices. WFP will scan for new devices attempting to access the network. An initial compliance check will be performed and devices not meeting the minimum will be blocked and/or redirected to these networks.

Personnel responsibilities

l. WFP personnel shall:

- protect their access credentials for IT systems and not disclose them; and
- always use WFP IT systems in accordance with the provisions in this document.

Supervisor responsibilities

m. Supervisors shall:

- request WFP systems access for personnel according to established procedures;
- inform the IT Service Desk or the local IT Officer when personnel leave their supervision, whether they have been transferred, have changed roles or have left the Organization; and
- periodically review system privileges granted to personnel. This involves a re-evaluation to determine whether current privileges are still needed to perform current job duties.

[9] Includes but not limited to PCs, laptops, tablet PCs, PDAs, smart phones, personal printers.
[10] http://mdm.wfp.org/ssp accessible using your active directory credentials.

IT personnel responsibilities

n. IT personnel shall ensure that appropriate action is taken to remove or update access rights when notification is received from supervisors or Human Resources on personnel moves or separations.

Administrator responsibilities

o. Administrators shall:

- be aware that the privileges they are granted place them in a position of considerable trust and only use their access privileges to carry out their work as described in their terms of reference; and
- use their access rights in accordance with the rules and policies outlined in this policy.

p. Administrators shall not:

- engage in any actions that may compromise their integrity or the integrity of the systems or networks they administer; and
- use administrative privileges to access or modify information, systems or configurations that do not fall under their area of responsibility unless express authorization has been granted by system owners.

8. **Access Codes and Password Policy**

a. Passwords are the entry point to WFP information systems and the front line of protection for user accounts. They are therefore pivotal in ensuring that WFP systems remain secure and the information within remains authentic and available.

b. A poorly chosen password may compromise the corporate network, implicating the individual whose password is compromised. Due diligence must therefore be exercised when selecting a password. All passwords are to be treated as sensitive, confidential WFP information.

c. Temporary, one-time passwords required to set up e-mail, LAN and WINGS accounts are sent by e-mail and should be changed by the personnel immediately. All WFP personnel are responsible for taking the appropriate steps, as outlined in Annex A, in selecting passwords. Change of set-up/initial passwords should be enforced.

d. Passwords for WFP accounts must be different than those used for non-WFP access, e.g. personal accounts, bank accounts, etc. Where possible, different passwords should be selected for each WFP account.

e. LAN, e-mail and WINGS passwords shall be changed every 90 days. Passwords cannot be re-used. Many password changes are system-enforced (e.g. LAN, e-mail, WINGS). That is, access to those systems will be blocked until a new password is selected.

f. Many information systems are subject to a timeout if sessions are inactive for 15 minutes and will require a valid password to unlock.

g. Requests for extraordinary access to system resources should be directed to the IT Security Officer through the IT Service Desk.

h. Anonymous and generically-named accounts to log into systems are not permitted.

i. For mobile devices, such as smart phones and tablets, authentication is mandatory prior to accessing the network. WFP Personnel must protect their devices and enable passcode lock features. Mobile devices can only access the WFP network if registered with the corporate Mobile Device Management portal.

Personnel responsibilities

j. WFP Personnel shall:

- be responsible for all their computer transactions;
- safeguard passwords and refrain from disclosing them to others or writing them down;
- immediately change passwords if it is suspected they may have been compromised;
- change passwords regularly, minimum when a system enforces such a change;
- be responsible for selecting passwords that are difficult to guess;
- password-protect all mobile devices and lock the device when left unattended; and
- lock the computer, log out or activate a password-protected screen saver when leaving a workstation unattended.

IT personnel responsibilities

k. IT personnel:

- will have a focal point responsible for maintaining a list of the various systems and administrators, and will provide this list upon request to the IT Security Officer;
- are responsible for ensuring that application development programs contain the appropriate security precautions for authentication by adhering to WFP release and development standards[11], and
- configure systems to lock in accordance with this policy.

9. Remote Network and Application Access

a. Remote access to WFP's systems and applications requires additional security measures such as additional authentication steps. IT personnel in offices will advise personnel on the local procedures for remote access.

b. Remote access to WINGS is forbidden on PCs, laptops and smart phones or PDAs that do not conform to the security requirements defined in Annex B.

[11] For more guidance, contact the IT Security Officer through the IT Service Desk.

Personnel responsibilities

c. Personnel shall:

- refer to and comply with the provisions on telecommuting of the HR Manual;[12]
- take special care to maintain the security of their VPN access credentials; and
- report any loss or theft of mobile devices to the relevant local IT device issuer in accordance with local procedures, referring to the MS Administrative Services Manual for further details on the loss or theft of devices.[13]

Supervisor responsibilities

d. Supervisors shall:

- ensure that personnel under their supervision are equipped with the required WFP-supplied hardware to carry out their assigned tasks.

10. **Internet Use Policy**

a. Access to the Internet is provided to personnel for the benefit of WFP. WFP expects that, in addition to other facilities, Internet access and electronic communications services will enable personnel to fulfil their job responsibilities better.

b. However, the Internet is also full of risks and inappropriate material, and this policy is intended to establish boundaries in order to promote productive Internet use and to protect the Organization's information and interests.

c. WFP maintains the right to analyze and momentarily store network traffic originating from any device connected to the corporate network. The monitoring system will record details like the source IP address, date, time, protocol and destination site and/or server - both for internal and Internet bound traffic.

d. The IT Division shall block access to Internet websites and protocols that are deemed inappropriate for WFP's corporate environment. Content filters will be reviewed and adjusted periodically.

e. Data and reports on internet usage that can be tracked to a specific workstation and/or named user will only be provided when an approved investigation is being carried out[14] –or if needed to support troubleshooting of severe bandwidth and system performance issues.

[12] http://wiki.wfp.org/human-resources-manual/index.php/V.7_Flexible_Working_Arrangements#8
[13] Stolen or lost mobile phones or smart phones must be reported in compliance with Directive AD2007/007, "Directive on Management of Telephone Services".
[14] For access to Personal Data, refer to the WFP Privacy and Data Protection Principles Section.

Prohibited Use

f. Personnel shall not use the WFP network or WFP issued equipment to view, download, save and/or send:

- pornographic material;
- material promoting sexual exploitation or discrimination, racism and violence;
- material that promotes discrimination on the basis of race, gender, national origin, age, marital status, sexual orientation, religion, health or disability;
- content that threatens and/or promotes violence and/or violent behaviour;
- material that constitutes gambling;
- Copyrighted material or material protected by intellectual property rights unless appropriate permission has been obtained from the owners; or
- illegal material[15].

g. WFP's computer services may not be used to display, store or send (by e-mail or any other form of electronic communication such as bulletin board, chat room, UseNet group) material that is: fraudulent, harassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise inappropriate or illegal.

h. Personnel shall not use WFP resources for personal gain, nor shall they send commercial messages[16] or material that promotes and/or advertises a business or other entity that does not benefit WFP in any way.

i. Use of unauthorized file sharing and download software (Ref. footnote 16) is prohibited due to the amount of network resources they consume, the security threats they bring, and the legal risks they pose. The Information Technology Division will monitor the use of such software and access to these services shall be blocked.

j. Personnel must not send any reports or data extracts containing sensitive data or other information with parameters, such as system access details, passwords and/or user account details, through the Internet unless the connection has been encrypted.

Frivolous Use

k. Frivolous use of the WFP network and Internet services is discouraged as it wastes computer resources and could lead to the unfair monopolization of these resources to the detriment of productivity and efficiency. Frivolous use includes, but is not limited to:

- browsing the Internet for non-work related purposes, including social networking, online gaming, chatting, video and audio streaming; and

[15] E.g. child pornography and copyright infringement.
[16] Prohibited activity includes communicating with WFP vendors or partners, etc about official WFP matters through the use of private channels. e.g. WFP personnel should not communicate with vendors using their private mail account to discuss procurement matters.

- subscribing to real-time or periodic automatic information distribution services, e.g. RSS feeds or newsletters, for information that is non-work related.

Acceptable Use

l. Acceptable use of the Internet means that personnel shall use the Internet responsibly, appropriately, ethically and legally. This includes to:

- obtain business information from commercial Web sites;
- access work-related news and current affairs information feeds;
- access online databases for information as needed;
- access emergency and disaster information sites as required;
- access personal bank accounts; and
- participate in self-advancement outside of scheduled working hours provided that such use is consistent with professional conduct.

m. WFP recognizes the need for personnel to use Internet services for personal use, especially in areas without adequate, publicly available infrastructure. In these instances, personnel can make personal use of corporate Internet services provided that such use:

- is limited to non-working hours (where possible);
- does not interfere with the operation of WFP's technical facilities by wasting resources or unfairly monopolizing them to the exclusion of others;
- does not diminish personnel's productivity in terms of work-related obligations; and
- does not violate the rules contained in this or any other applicable policy.

n. The above listed standards are designed to ensure the use of Internet in a safe and responsible manner and to guarantee adequate bandwidth and infrastructure resources needed to access business critical corporate systems.

Personnel responsibilities

o. Personnel must be aware that not all information available on the Internet may be reliable. While the web sites of official bodies can be considered authentic and valuable reference sources, there are numerous sites of a personal nature or with suspected credentials that should be treated with caution. The reliability and accuracy of the information contained therein must be confirmed from other sources.

p. Personnel shall:

- ensure that the Internet is used in line with the provisions of this policy and that their Internet-based activities are compliant with the, "Standards of Conduct for the International Civil Service"[17]; and

[17] http://icsc.un.org/resources/pdfs/general/standardsE.pdf

- understand that Internet access is for the purpose of increasing productivity and not for engaging in non-WFP business activities.

Supervisor responsibilities

q. Supervisors retain discretion in what constitutes excessive personal use of the Internet by personnel under their supervision and may request corrective action be taken by IT.

11. E-mail and Instant Messaging Security Policy

a. E-mail is now one of WFP's primary business communication means. The authentication and security model used by the corporate e-mail system can guarantee message authenticity and non-repudiation within the WFP network. Personnel must not use the WFP e-mail system for purposes that are illegal, unethical or harmful to the Organization.

Personnel responsibilities

b. Personnel shall:

- refer to and comply with Directive OD2010/001, "Directive on the Use of WFP Corporate E-mail and Other Electronic Messaging Services";
- use only WFP e-mail accounts, not personal accounts, to send confidential and strictly confidential information; and
- use WFP e-mail responsibly and appropriately.

12. Mobile and portable devices

Personnel with a need to use their personally-owned IT equipment for work purposes must be explicitly authorized to do so. The equipment will have to meet the specifications in the WFP IT standards and the security requirements specified in this document.Use of personal equipment is associated with a number of information security risks. By connecting their personally-owned IT equipment to WFP' network, WFP personnel grant WFP the right to access those devices, under the conditions established in paragraphs d) and e) of section 19 of this policy. Authorization requests can be granted or rejected if deemed not appropriate.

13. Voice over IP (Internet telephony)

Voice over IP and videoconferencing services are provided to all personnel by Lync. Details can be found in the Telecommunications directive OST2014/001.

14. Cloud computing

Cloud computing is a means by which an organization secures access to a shared pool of computing resources as and when they are needed. The resources might include networks, servers, storage, applications and services via a cloud-computing provider who will

manage these resources for the organization. Acquisition of cloud services must be in line with the policies and procedures spelt out in the "WFP Cloud Computing position paper"[18].

15. **Security Threats**

a. A security threat exploits system vulnerabilities and can result in the severe disruption of IT services, cause hardware and system failure, cause information loss, compromise information integrity and confidentiality, and interrupt WFP business. Such security threats may be malicious, provoked by viruses, worms, phishing attacks, etc., or non-malicious, consisting of unintentional errors such as a data entry or programming error, which can create system vulnerabilities.

b. Some malicious acts may request personnel to verify their passwords or click on a link to update their accounts. WFP will never send e-mails requesting personnel to provide their credentials. However authentic these may look, they may be social engineering techniques designed to compromise authorized user credentials. Personnel are responsible for maintaining the integrity of their credentials and must never disclose their passwords or other personal information in response to such messages.

c. Unsolicited emails from other sources may also contain phishing or social engineering techniques which attempt to obtain privileged information by pretending to originate from authorized sources.

d. Viruses can be found in files which are downloaded from websites or emails, such as embedded executables[19]. When such a file is opened, the virus will be launched and can spread through the computer or network causing damage to data or other systems. As such, unauthorized download of files from the Internet are <u>not</u> permitted and may be blocked.

e. It is relatively easy to fake the identity of another Internet user; as a result, personnel must not rely on the alleged identity of a correspondent via the Internet unless the identity of this person is confirmed. If in doubt, Country Office personnel are to contact their local IT officer and HQ personnel can contact the IT Service Desk.

f. Social networks can expose personnel to personal security risks, e.g. impersonation, identity theft and cyber-bullying.

g. Should personnel need to download files from the Internet; exceptions can be made on a case-by-case basis. Field personnel should seek clearance from their local IT Officer or Regional IT Officer while personnel at HQ should send their requests to the IT Service Desk, specifying the site and file intended for download.

h. The use of file-sharing software[20] is prohibited as it may allow remote access from an unauthorized user, contain malicious code and compromise the WFP network. Additionally, use of such utilities exposes the personnel and WFP to the legal risks

[18] WFP Cloud computing position paper
http://docustore.wfp.org/stellent/groups/public/documents/govman/wfp264704.pdf
[19] Files that end with ".exe" and contain programs which run when clicked on.
[20] BitTorrent, uTorrent, Shareaza, BitComet are examples of forbidden file sharing software.

associated with copyright infringement[21]. WFP Box - a private cloud service for sharing large files with personnel and externals should be used as a safe alternative to commercial offerings.

i. Personnel should be aware that fax machines send and receive information using unsecured public fax line services and the location of recipient fax machines could potentially expose sensitive documents. This means that information sent by fax could be intercepted and as such other means of information transmission should be used where possible.

j. Network vulnerability testing, which seeks to identify weaknesses in network security, must only be carried out with the authorization of the IT Security Officer.

Personnel responsibilities

k. Personnel shall:

- be aware of the security threats detailed above;
- use only trusted sources for data and programs;
- not knowingly introduce a computer virus into WFP computers;
- first scan portable storage devices with anti-virus and security software before browsing the contents; and
- immediately call the IT Service Desk or local IT Officer if it is suspected that their workstation or environment has been compromised by a security threat.

16. **Physical Security of Information Systems**

a. The aim of this policy is also to protect WFP IT equipment from misuse, theft, loss, unauthorized access, and environmental hazards, whether on or off WFP premises.

Personnel responsibilities

b. Personnel shall:

- refer to and comply with the Asset Management Manual [22]which defines the policies and procedures for the management of inventory items including IT equipment;
- store flash disks and other portable storage media out of sight when not in use, locking them up if they contain highly sensitive or confidential data and keeping them away from environmental hazards such as heat, direct sunlight, and magnetic fields;
- exercise care to safeguard the IT equipment assigned to them; and
- immediately report any loss, theft or damage of equipment to their local IT device issuer in accordance with local procedures.

[21] Current "IT Standards for End-User Hardware and Software" can be found in DocuStore through WFPGo.
[22] http://wiki.wfp.org/assetmanual/index.php/Main_Page

Supervisor responsibilities

c. Supervisors shall ensure that personnel have been assigned adequate resources to comply with the rules for physical security of Information Systems.

IT personnel responsibilities

d. IT personnel shall:

- install core computing equipment within a secured area with physical access control, air-conditioning and fire protection;
- protect critical IT equipment by an uninterruptible power supply (UPS);
- protect telephone and leased lines by a properly grounded lightening arrestor;
- perform all IT equipment installations, disconnections, modifications, and relocations;[23]
- store licensed software and associated documentation and peripheral media in lockable cabinets and limit access to authorized IT personnel; and
- place LAN and system administrator offices external to the server room and data centre environment, where possible.

17. **Copyrights and License Agreements**

a. It is WFP policy to comply with copyright laws and regulations governing intellectual property, as applicable.

b. WFP and its personnel are legally bound to comply with International Copyright and proprietary software license agreements. Non-compliance can expose WFP and responsible personnel to civil and/or criminal liabilities.

c. This policy applies to all software that is owned by WFP, licensed to WFP, or developed using WFP resources by personnel or vendors, and it applies to any material downloaded from the Internet or otherwise comes into WFP-owned equipment and systems.

d. Software installed on PCs and servers must be legally acquired with a valid license agreement and must be in compliance with the IT End-User and System Software Standardisation Directive, ODI2010/001.

Personnel responsibilities

e. Personnel shall:

- refer to the information note on current standard versions of software, which is updated annually;[24]
- install only software that is licensed to or owned by WFP on WFP computers;
- shall not install, copy or download software unless authorized by IT personnel and complies with licensing agreements;

[23] This does not apply to temporary moves of portable computers.
[24] Current “IT Standards for End-User Hardware and Software” can be found in DocuStore through WFPGo.

- where material contained in magazines, journals, newsletters and other publications is protected by copyright, permission must be obtained from the relevant copyright owner(s) prior to making copies;
- shall send all requests for needed software to the IT Service Desk or to their local IT officer; and
- shall not utilize copyrighted material in any way that contravenes the owner's copyright privileges.

IT Security Officer responsibilities

f. The IT Security Officer will:

- recommend and oversee the implementation of systems and technologies to monitor and, where necessary, restrict access to intellectual property and to proprietary and copyrighted material, and
- actively monitor compliance to the provisions of this policy and report violations found.

IT personnel responsibilities

g. IT personnel shall be responsible for:

- maintaining records of software licenses owned by WFP;
- checking the Organization's computers periodically to verify that only authorized software is installed;
- uninstalling or deleting unauthorized and/or unlicensed software;
- confirming requests for non-standard software with the Policy, Strategy and Architecture branch of IT; and
- reporting potential violations, as appropriate, to the IT Security Office.

18. **Disposal of old IT equipment**

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other components could possibly contain corporate WFP data, some of which might be considered sensitive or classified as confidential. All storage mediums must be properly erased before being disposed of. Technology assets that have reached the end of lifecycle or for any reason is no longer in working condition should be disposed of following the procedures described in the OST Information Note – Guidelines for Disposal of IT Material[25].

[25] Guidelines for the disposal of IT Materials
http://docustore.wfp.org/stellent/groups/gap_content/documents/govman/wfp245503.pdf

19. **WFP Privacy and Data Protection Principles**

a. WFP takes the privacy of its personnel seriously. Information about activity on WFP systems is restricted to appointed personnel whose roles and responsibility in the access and devolution of that information are clearly defined.

b. The following principles have been adopted to govern the use, collection, and transmittal of Personal Data[26], except as specifically provided by this Policy or as required by WFP rules:

i. Personal Data shall only be processed fairly and lawfully;
ii. Personal Data shall be obtained only for specified, explicit, lawful, and legitimate purposes, and shall not be further processed in any manner incompatible with those purposes;
iii. Personal Data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or processed;
iv. Personal Data shall not be collected or processed unless one or more of the following apply:

- the Data Subject[27] has provided consent;
- processing is necessary for the performance of a contract directly with the Data Subject, or to which the Data Subject is a personnel of a party;
- processing is necessary for compliance with WFP legal obligation or investigation purposes;
- processing is necessary in order to protect the vital interests of the Data Subject;
- processing is necessary for legitimate interests of WFP or by the third party or parties to whom the Data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the Data Subject;

v. appropriate physical, technical, and procedural measures shall be taken to prevent and/or to identify unauthorised or unlawful collection, processing, and transmittal of Personal Data; and
vi. prevent accidental loss or destruction of, or damage to, Personal Data.

c. For corporate security risk compliance, WFP reserves the right to log any system access and activity on its computer systems and network infrastructure. Logging includes, but is not limited to:

- the content of end-point devices (private and corporate owned);
- chat rooms, newsgroups and Internet sites visited;
- file and media downloads;

[26] Personal data refers to data that can be used to fully identify an individual either when used alone or coupled with other information available elsewhere.
[27] Data Subject is a term commonly used in data protection and privacy laws to mean an individual who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, or a unique identifier.

- network traffic; and
- all communication sent and received electronically.

d. System maintenance and trouble-shooting logs may be monitored. E-mail contents, however, will not be accessed without express permission from the personnel, or clearance from senior management.

e. Monitoring of network and computer usage activities and the retrieval of related information (including e-mail, instant messaging and internet browser details) is allowed when a legitimate corporate need exists, such as:

- suspicion of corporate policy violation or illegitimate activity;
- maintenance of computer systems; and
- unavailability of personnel.

f. Monitoring and retrieval of information and staff communications including exceptional cases where system access is necessary, for example, when an investigation or an investigative review is being carried out by the WFP Office of Inspector General, clear and authenticated written instruction will come from the Deputy Executive Director specifying the access needs. The IT Security Officer is responsible for the technical implementation to ensure this technical capability and observing confidentiality in this process.

20. **Divisional responsibility**

g. The Chief Information Officer & Director, IT Division is responsible for:

- overall implementation of the policy;
- monitoring the execution and impact of the policy on the Programme;
- reporting annually to the Executive Director on its implementation;
- compliance with relevant internal rules and legislation on data protection and Internet access.

21. **Violations**

h. Apparent violations should be brought to the attention of the chief of the relevant office and the Deputy Executive Director & Chief Operating Officer. The Offices of Human Resources and the Office of Inspector General will be notified, as warranted.

Ertharin Cousin
Executive Director

References

OD2010/001 Directive on the Use of WFP Corporate E-mail and Other Electronic Messaging Services
http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp215287.pdf

AD2006/006 Directive on Records Retention Policy in WFP
http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp090363.pdf

HR Manual provisions on Telecommuting
http://wiki.wfp.org/human-resources-manual/index.php/V.7_Flexible_Working_Arrangements#8

Asset Management Manual
http://wiki.wfp.org/assetmanual/index.php/Main_Page

Standards of Conduct for the International Civil Service
http://icsc.un.org/resources/pdfs/general/standardsE.pdf

CP2010/001 Directive on Information Disclosure
http://docustore.wfp.org/stellent/groups/public/documents/cd/wfp220970.pdf

Annex A

LAN Access Statement

Prior to logging into the WFP LAN and webmail, personnel shall be presented with the following statement:

> "By logging onto any WFP IT system users affirm that they have read, understood and acknowledge the Corporate Information and IT Security Policy. Kindly direct any queries to the IT Service Desk."

Security Threats: Symptoms of Infections

Though infections have different symptoms, the following list provides some clues:

- the PC restarts spontaneously;
- the PC freezes;
- a blue text screen appears; or
- system messages on the screen appear concerning memory that cannot be read, accessed or written to.

Access Codes and Password Policy: Password Construction Guidelines

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords.

Strong passwords:

- contain both upper and lower case characters (that is, a-z, A-Z);
- have digits and punctuation characters as well as letters (that is, 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- are pass phrases that contain at least fifteen alphanumeric characters and multiple words, e.g. Ohmy!1stubb3dmyt0e:-(.

Passwords should NOT:

- contain less than eight (8) characters;
- contain words found in a dictionary (English or foreign);
- be based on personal information, such as birthdays, family names, etc.; or
- be common usage words such as:
    - computer terms, commands, companies, hardware or software;
    - the word *WFP*, common place names or any derivation;
    - word or number patterns like *aaabbb*, *qwerty*, *zyxwvuts*, *123321*, etc.;
    - any of the above spelled backwards; and
    - any of the above preceded or followed by a digit (e.g. secret1, 1secret).

For services where the use of a Passphrase is required, these should contain no less than 15 (fifteen) characters and must be complex.

Personnel should NOT:

- write passwords down or store them on disk or on-line without encryption;
- share passwords with or hint at them to anyone, including family members, supervisors, co-workers and personal assistants;
- reveal passwords to anyone;
- reveal passwords in questionnaires or security forms to family members, or
- use the "Remember Password" feature of applications and browsers.

Annex B

Authorized environments, equipment and services for information storage and system access.

1. Confidential and strictly confidential material must be handled in ways that minimizes loss or damage and must not be stored or shared on personal e-mail, media such as flash disks or Internet based storage services. Confidential and strictly confidential information must only be stored on one of the following:

   - protected WFP shared network drives and teamwork services.
   - internal and/or external cloud computing storage services, but **only** if approved by the IT Division;
   - WFP-issued hardware; and
   - WFP-issued portable media provided information is secured using WFP provided encryption techniques.

2. Personnel may occasionally or on an emergency basis need access to WINGS and other corporate systems using equipment not issued by WFP. Accessing these systems from non-WFP equipment means minimum security requirements cannot be enforced. Examples of such equipment are the home PC, personal laptop or tablet PC.

3. Personnel using non-WFP issued equipment are required to install software called 'AnyConnect' which provides an additional layer of security.

4. The software can be downloaded and installed in the following way:

   - open the website https://mobile.wfp.org; or
   - click on the link 'Cisco AnyConnect VPN client.

   This will automatically launch and install the software. Additional instructions can be found here:
   http://docustore.wfp.org/stellent/groups/public/documents/ko/wfp202222.pdf

Annex C

WFP Data Encryption guidelines:

a. All confidential or strictly confidential information should be stored on a secure WFP network server with restricted access.

b. Desktops, laptops, removable storage devices and smart devices should not be used for long-term/permanent storage of sensitive information.

c. Any portable computing device that contains information classified by WFP as confidential or strictly confidential should have such data encrypted if used away from premises.

d. When properly implemented, data encryption will provide an enhanced level of protection against unauthorized access and use in the event of theft, loss or interception. This extra safeguard measure should apply both to data at rest and data in motion.

e. Encryption may not be applicable in all situations. Therefore, use encryption on data that is classified as confidential or strictly confidential and/or when encryption is mandated.

f. WFP will only endorse the use of encryption technologies based on standard validated algorithms (e.g., DES, RSA, and IDEA) – and systems configured to use 128 bit encryption cipher keys as a minimum requirement.

g. Effective key management is a crucial element for ensuring the security of any encryption system. Key management procedures must ensure that authorized users can access and decrypt all encrypted data using controls that meet operational needs and comply with data retention requirements. Key management should be automated as much as possible and include procedures for recovery and decryption of data in case of lost keys.

h. Technology, tools, algorithms and key length requirements will be reviewed periodically and upgraded as technology allows. Guidance on the implementation of encryption within WFP is available directly from the IT Security Officer.