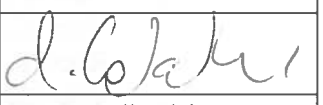
ECDC

Internal policy on the use of ICT equipment at ECDC	
Number	ECDC/ADM/001
Consultation: EXC	
Author: Stefan Fassbender	
Approval : Director	
Adoption by MB :	not applicable
Date issued (effective date):	15.01.2007
Review date:	31.12.2008

Purpose

This policy provides information security instructions applicable to all users that use ECDC personal computers and other Information and Communication Technology. All ICT users are expected to comply with this policy when using ICT equipment at ECDC.

Scope

This policy applies to all staff, personnel, contractors, consultants, interims, and Seconded Experts (generalized as users), who use the ICT equipment at ECDC's computing or networking resources. The policy applies to all those who use the Internet, computer facilities and represent themselves as being connected in some way with ECDC

Background/legal base

Users of any ICT system of ECDC must receive permission in writing to use the ICT system from ECDC. Access to the computing resources provided by ECDC is subject to the acceptance of the individual declaration given in an Individual declaration. All users shall be duly notified that use of the computing resources of ECDC for the first time constitutes acceptance of that declaration.

Description

The policy provides information security instructions applicable to all users that use ECDC personal computers and other Information and Communication Technology. It provides general information for all ICT systems e.g. in terms of permissions, privacy and reporting of security incidents and specific rules how to use the personal computer, the Internet and messaging and communication systems.

Content

1 Introduction

1.1 Purpose of this policy

A large portion of ECDC business and operations is conducted with personal computers, including portable computers, handheld computers, personal digital assistants, telephones and similar computers and other Information and Communication Technology equipment dedicated to a single user's activity. Protection of personal computers and the information handled by these systems is an essential part at ECDC. To this end, this policy provides information security instructions applicable to all users that use ECDC personal computers and other Information and Communication Technology. All ICT users are expected to comply with this policy as a condition of continued employment.

Beyond this policy all ICT users at ECDC are requested to use the ICT equipment and handle the information of ECDC in a cautious and responsible manner to protect ECDC's assets and interests.

1.2 Scope

This policy applies to all staff, personnel, contractors, consultants, interims, and Seconded Experts (generalized as users), who use the ICT equipment at ECDC's computing or networking resources. The policy applies to all those who use the Internet, computer facilities and represent themselves as being connected in some way with ECDC. All of these users are expected to be familiar with and fully comply with this policy. Questions about the policy should be directed to the HoU Administration or the Information Security officer. Breaches of this policy may give rise to disciplinary proceedings.

The present policy is focused on systems handling non-Classified information. The regular infrastructure of ECDC is not designed for the handling, storage or transmission of *confidential* or *secret* information.

2 General rules

2.1 Permission to use ICT Systems

Users of any ICT system of ECDC must receive permission in writing to use the ICT system from ECDC. Access to the computing resources provided by ECDC is subject to the acceptance of the individual declaration given in the Annex 4.2 Individual declaration. All users shall be duly notified that use of the computing resources of ECDC for the first time constitutes acceptance of that declaration.

All users must receive additional permission in writing to use information systems that allow access to *confidential* and *secret* information from the ECDC,

Users must bear in mind that the regular computer systems are not suitable for storing and handling information with *confidential* or *secret* rating. Users must be aware that the information they are allowed to store or handle on each system they can access, including the workstations or portable computers supplied by ECDC is public or restricted only. If there is a need to store or handle information of a higher classification rating, users must notify the Help Desk or the Information Security officer. For the handling of personal data the Data protection officer should be involved.

2.2 Business use only

Business Use Only—As a rule, ECDC computer and communication systems are intended to be used for business purposes only. Use of computing resources for private purposes must be limited and it shall not run counter to the interests of the service or hamper the smooth running of the Agency. Offensive material that might cast ECDC in a bad light, including sexist, racist, violent, or other content, is strictly forbidden from all ECDC personal computers.

2.3 Exceptions on privacy

Management Review— The information stored in the computing facilities of ECDC remains the property of ECDC. In accordance with [2] at any time and without prior notice, ECDC management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through ECDC computers, without prior notification and without the presence of the staff member to whom the equipment has been supplied for serving the professional interests of ECDC. This information shall not be publicly available and shall always be protected according to the terms of [3,4,5].

Logging—ECDC routinely logs the web sites visited, files downloaded, time spent on the Internet, and related information. Head of Units may receive reports

of such information. This information shall not be publicly available and shall always be protected according to the terms of [3,4,5].

Blocking Sites and Content Types—The ability to connect with a specific web site or other external service does not in itself imply that users of ECDC systems are permitted to visit that site or use this service. ECDC may, at its discretion, restrict or block the downloading of certain file types or services that are likely to cause network service degradation or other impact on the operational business of ECDC. These file types include graphic and music files.

2.4 Reporting security problems

Custodians For Equipment—The primary user of a personal computer is considered a Custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a Custodian must promptly inform the Head of ICT. With the exception of portable machines, personal computer equipment must not be moved or relocated without the knowledge and approval of ICT group.

Notification Process—If sensitive ECDC information is lost, disclosed to unauthorized parties, or suspected of either, the Information Security officer must be notified immediately. If any unauthorized use of ECDC information systems has or is suspected of taking place, the Information Security officer must be notified immediately. Whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, helpdesk and the Information Security officer must be notified immediately. All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages must be immediately reported to the help desk. The specifics of security problems must not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports—Users in receipt of information about system vulnerabilities must forward it to the Information Security officer, who then will determine what if any action is appropriate. Users must not personally redistribute system vulnerability information to other users.

Suppress reporting - Actions aiming at preventing or obstructing reporting of security incidents to the appropriate persons are forbidden and may be subject to disciplinary actions.

2.5 Intellectual Property Rights

Copyright Protection—Making unauthorized copies of licensed and copyrighted software, even if for "evaluation" purposes, is forbidden. ECDC permits reproduction of copyrighted materials only to the extent legally considered fair use or with the permission of the author or Owner. If users have any questions about the relevance of copyright laws, they must contact the ECDC legal advisor. Unless they receive information to the contrary, users must assume that software and other materials are copyrighted.

2.6 User Identification and Authentication

Userids - All users are assigned user identification values (userids), which may be used for making users accountable for their actions. A user may be given different userids for different computer systems but any userid shall be unique on each computer system.

Sharing passwords - Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. Information Technology staff must never ask users to reveal their passwords. If users need to share computer resident data, they should utilize message forwarding facilities, public directories on local area network servers, groupware databases, and other authorized information-sharing mechanisms.

Prevent password disclosure - To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess. Users are reminded that by revealing their passwords, they may undertake the responsibility of actions carried out by other people. Users must choose passwords that are difficult to guess. Words that can be found in dictionaries and personal details, such as names, addresses and dates of birth, must not be used in constructing passwords. Guidelines for constructing good passwords are given in the Annex Guidelines for constructing good passwords.

Suspect of password compromise - If a user finds out or suspects that their password has somehow been compromised, they should immediately construct a new password and report the incident to the Local Help Desk service.

Transmission of password - Users must refrain from transmitting their passwords through e-mail systems or other electronic or conventional communication means like regular mail.

Noting passwords - Users should avoid writing down their passwords; should a password be written down, it should be well protected from unauthorised access.

Authentication token - The authentication tokens provided by the ECDC to its staff or contractors remain the property of ECDC.

Loss or damage of tokens - The users are responsible for protecting the authentication tokens against loss or physical damage. Should a token been lost or damaged, the user must report the incident to the helpdesk.

Administrative passwords – A regular updated print out of the passwords of central systems for higher privileges should be stored in a sealed envelope in the bank safe of ECDC.

2.7 Others

No Default Protection—Users using ECDC information systems or the Internet must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, users must not send information over the Internet if they consider it to be confidential or private.[1]

Testing Controls—Users must not test or probe security mechanisms at either ECDC or other Internet sites unless they have obtained written permission from the Information Security officer. The possession or the usage of tools for detecting information system vulnerabilities, or tools for compromising information security mechanisms are prohibited without the advance permission of the Information Security officer.

[1] SI2 is not using the Internet as transport medium but Testa.

3 Specific rules

3.1.1 Rules for the use of the personal computer

3.1.1.1 Change control

Changes to application software—ECDC has a standard list of permissible software packages that users can run on their personal computers [*link to standard conf.]*.Users must not install other software packages on personal computers without obtaining advance permission from the Head of ICT. Users must not permit automatic software installation routines to be run on ECDC personal computers unless these routines have been approved by the Head if ICT. Unless separate arrangements are made with the Head of ICT, upgrades to authorized software will be downloaded to personal computers automatically. Unapproved software may be removed without advance notice to the involved user.

Changes to operating system configurations—On ECDC-supplied computer hardware, users must not change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they must be performed by help desk personnel, in person or with remote system maintenance software.

Changes to hardware—Computer equipment supplied by ECDC must not be altered or added to in any way (including the network connection, connection of private USB sticks, cameras etc.) without the prior knowledge of and authorization from the Head of ICT.

3.1.1.2 Handling and Disposal of Printouts

Leakage of information - Users are reminded that printing and disposal of documents may result in leakage of sensitive information.

Unattended print out - Users must refrain from printing documents containing *Restricted* information on unattended printers to which physical access is not controlled. Staff members shall always protect printouts containing *Restricted* information against unauthorized disclosure. In particular, staff members shall clean their working areas so that printouts containing *Restricted information* are not accessible to unauthorized persons. Print jobs of *Restricted* information that can't be printed (e.g. because there is a jam of the printer) should be deleted in the print queue.

Disposal of restricted printouts - Printouts containing *Restricted* information should be binned in the red disposal boxes.

Higher Classified information printout – Information with the classification of *Confidential* and *Secret* should neither be handled on the regular ECDC computer systems nor printed on the regular printers. Handling and printing of *Confidential* and *Secret* information is subject to a dedicated policy for handling of classified information.

3.1.1.3 Electronic viruses

Virus program installed—All personal computers must continuously run the current version of antivirus detection software. The current version of this antivirus software is installed on each personal computer when the machine is connected to the ECDC internal network. Users must not abort this software or download process of new virus pattern. In case of suspect the AV software not to run properly or not to be up to date Helpdesk should be informed.

Decompression before checking—Externally-supplied floppy disks, CD-ROMs, and other removable storage media must not be used unless they have been checked for viruses. Attachments to electronic mail must not be executed or opened unless they have been checked for viruses[1]. Externally-supplied, computer-readable files, software programs, databases, word processing documents, and spreadsheets must be decompressed prior to being subjected to an approved virus-checking process. If the files have been encrypted, they must be decrypted before running a virus-checking program.

Eradicating viruses—Users must not attempt to eradicate a virus without expert assistance. If users suspect infection by a virus, they must immediately stop using the involved computer, physically disconnect from all networks, and call the Help Desk. If the suspected virus appears to be damaging information or software, users must immediately turn off the personal computer.

Playing with viruses—Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any ECDC computer system.

3.1.1.4 Use of facilities

Use of personal equipment—Users must not bring their own computers, computer peripherals (including USB disk drives etc), or computer software into ECDC facilities. Users must not use their own personal computers for production ECDC business. Writing Emails or reports is not considered production ECDC business for purposes of this policy.

Modems, wireless devices—Modems or wireless network extenders inside or attached to ECDC office desktop personal computers are not permitted.

Installation Of communications lines—Users must not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not obtained approval from the Head of ICT.

Establishing networks—Users must not establish electronic bulletin boards, local area networks, modem connections to existing internal networks, Internet commerce systems, or other multi-user systems for communicating information.

Internet—As a matter of policy, inbound Internet connections to ECDC personal computers is forbidden unless these connections employ an approved virtual private network (VPN) software package deployed by the IT group of ECDC.

[1] Our email system checks for viruses, but web based private email services usually don't.

Access Control—All ECDC personal computers must run an access control package. Typically these packages require a fixed password at the time a personal computer is booted and again after a certain period of no activity. If sensitive information resides on a personal computer, the screen must immediately be locked or turned off, whenever a worker leaves the location where the personal computer is in use.

3.1.2 Rules on the use of the Internet

3.1.2.1 Information Integrity

Information Reliability—All information acquired from the Internet must be considered suspect until confirmed by separate information from another source. Before using free Internet-supplied information for operational decision-making purposes, users must corroborate the information by consulting other sources.

Virus Checking—All non-text files downloaded from non-ECDC sources through the Internet must be screened with current virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software must be tested on a stand-alone, non-production machine that has been recently backed up. Downloaded files must be decrypted and decompressed before being screened for viruses. The use of digital signatures to verify that a file has not been altered by unauthorized parties is recommended, but this does not assure freedom from viruses, Trojan horses, and other problems.

Software Downloading—ECDC will implement an automatic software distribution system to install the latest release of licensed software on ECDC computers. A separate system is used to automatically trace all software resident on these same systems. As specified under 3.1.1.1, users must not download or install software on their ECDC-supplied computers, whether the software was downloaded from the Internet or procured elsewhere.

User Anonymity—Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any ECDC electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. If users have a need to employ remailers or other anonymous facilities, they must do so on their own time, with their own information systems and Internet service provider accounts. Use of anonymous FTP logons, anonymous UUCP logons, HTTP or web browsing, and other access methods established with the expectation that users would be anonymous are permissible.

Authentication for Internet Access- Access to the Internet services requires the users to authenticate themselves to the systems of ECDC used for accessing the Internet. Usually this authentication takes place automatically via single sign on. In case of trouble please contact helpdesk. Internet users shall not take up the identities of other users or non-existing identities while using any Internet service through the computing and network resources supplied by ECDC.

3.1.2.2 Information Confidentiality

Information Exchange—ECDC software, documentation, and all other types of internal information must not be sold or otherwise transferred to any ECDC counterpart for any purposes other than business purposes expressly authorized by management. Exchanges of data between ECDC and any third party must not proceed unless a written agreement has been signed. Such an agreement must specify the terms of the exchange, and the ways that the software or data is to be handled and protected.

Posting Materials—Users must not post unencrypted ECDC material on any publicly-accessible Internet computer that supports anonymous FTP or similar publicly-accessible services, unless the posting of these materials has been approved by the Director. ECDC internal information must not be placed in any none ECDC computer.

Message Interception—ECDC confidential, secret, proprietary, or private information must not be sent over the Internet unless it has been encrypted by approved methods.

Security Parameters—Unless a connection is known to be encrypted, credit card numbers, telephone calling card numbers, fixed logon passwords, and other security parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form (e.g. Email is not a realiabe medium).

Encryption software - Encryption processes initiated by ECDC are permissible if they are provided by ECDC ICT group.

3.1.2.3 Public Representations

External Representations—Users may indicate their affiliation with ECDC in mailing lists, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for example through an electronic mail address. In either case, whenever users provide an affiliation, unless they have been expressly designated as a spokesperson of ECDC, they also must clearly indicate the opinions expressed are their own, and not necessarily those of ECDC. If an affiliation with ECDC is provided, political advocacy statements and cooperation agreements also are prohibited unless they have been previously cleared by the Director or the ECDC spokesman. All representations on behalf of ECDC must be cleared by the Director or the ECDC spokesman.

Appropriate Behavior—Whenever any affiliation with ECDC is included with an Internet message or posting, written attacks are strictly prohibited. In general users must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

Removal Of Postings—Those messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, that include an implied or explicit affiliation with ECDC, may be removed if management deems them to be inconsistent with ECDC interests. Messages in this category include political

statements, religious statements, cursing or other foul language, and statements viewed as harassing others based on race, creed, color, age, sex, physical handicap, or sexual orientation. The decision to remove electronic mail must be made by the Director. When practical and feasible, individuals responsible for the message will be informed of the decision and given the opportunity to remove the message themselves.

Disclosing Internal Information—Users must not publicly disclose internal ECDC information through the Internet or otherwise that may adversely affect the ECDC Member States or partner relations, or public image ..

Inadvertent Disclosure—Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Usenet, and related public postings on the Internet. Before posting any material, users must consider whether the posting could put ECDC at a significant competitive disadvantage or whether the material could cause public relations problems. Users should keep in mind that several separate pieces of information can be pieced together to form a picture revealing sensitive information that then could be used against ECDC. Users must never post on the Internet the specific computer or network products employed by ECDC.

3.1.2.4 Access Control

Inbound User Authentication—All users wishing to establish a real-time connection with ECDC internal computers through the Internet must employ a virtual private network (VPN) product that will be implemented by the ICT group. This VPN product also authenticates remote users at a firewall level before permitting access to the ECDC internal network.

Remote Machine Security—Users who have not installed required software patches or upgrades, or whose systems are virus-infested must be disconnected automatically from the ECDC network until they have reestablished a secure computing environment. ECDC Laptops that have been disconnected to the ECDC infrastructure for more than 1 month should be taken to helpdesk for update prior the connection to the ECDC network.

Restriction Of Third-Party Access—Inbound Internet access privileges must not be granted to third-party vendors, contractors, consultants, interims, outsourcing organization personnel or other third parties unless the relevant system manager determines that these individuals have a legitimate business need for such access. These privileges must be enabled only for specific individuals and only for the time period required to accomplish approved tasks.

Browser User Authentication—Users must not save fixed passwords in their web browsers or electronic mail clients. These fixed passwords must be provided each time that a browser or electronic mail client is invoked. Browser passwords may be saved if a boot password must be provided each time the computer is powered up, and if a screen saver password must be provided each time the system is inactive for a specified period of time.

Data Aggregators—Users must not provide their Internet user IDs and passwords to data aggregators, data summarization and formatting services, or any other third parties.

3.1.3 Rules on the use of the messaging and communication systems

3.1.3.1 General rules

ECDC Property—As a productivity enhancement tool, ECDC encourages the business use of electronic communications systems, notably the Internet, electronic mail, and fax. Unless third parties have clearly noted copyrights or some other rights on the messages handled by these electronic communications systems, all messages generated on or handled by ECDC electronic communications systems are considered to be the property of ECDC.

Message Forwarding—Electronic communications users must exercise caution when forwarding messages. ECDC sensitive information such as *Restricted* information must not be forwarded to any party outside ECDC without the prior approval of a Head of Unit. Messages sent by outside parties must not be forwarded to other third parties unless the sender clearly intended this and such forwarding is necessary. In general, forwarding of messages sent by outsiders to other third parties can be done only if the sender expressly agrees to this forwarding. Automatic message forwarding to e-mail addresses that do not belong to ECDC is not allowed. Message forwarding should be used when there is a need to allow staff members to read the e-mail of their colleagues that are absent or unable to access their e-mail account.

Purging Electronic Messages—Messages no longer needed must be periodically purged by users from their personal electronic message storage areas.

Use At Your Own Risk—Users access the Internet with ECDC facilities at their own risk. ECDC is not responsible for material viewed, downloaded, or received by users through the Internet. Electronic mail systems may deliver unsolicited messages that contain offensive content.

3.1.3.2 Information Integrity and Confidentiality

Authorized Usage—ECDC electronic communications systems generally must be used for business activities only.. Use of computing resources for private purposes must be limited and it shall not run counter to the interests of the service or hamper the smooth running of the Agency. ECDC electronic communication systems must not be used for charitable fund raising campaigns, political advocacy efforts, religious efforts, private business activities, or personal amusement and entertainment. News feeds, electronic mail mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to both ECDC business and the duties of the receiving users. Users are reminded that the use of information system resources must never create the appearance or the reality of inappropriate use and there are clear rules on privacy (see 3.1.3.5 Exceptions on privacy).

Labeling Electronic Mail Messages—All electronic mail messages containing sensitive information must include the appropriate classification (*Restricted*) in the header. This label will remind recipients that the information must not be disseminated further, or be used for unintended purposes, without the proper authorization.

Contents Of Messages—Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, partners competitors, or others. Such remarks, even when made in jest, may create legal problems such as trade libel and defamation of character. It is possible that these remarks would later be taken out of context and used against ECDC. To prevent these problems, users must concentrate on business matters in ECDC electronic communications.

Harassing Or Offensive Materials—ECDC computer and communications systems are not intended to be used for, and must not be used for the exercise of the users' right to free speech. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Users who receive offensive unsolicited material from outside sources must not forward or redistribute it to either internal or external parties, unless this forwarding or redistribution is to the ECDC Human Resources group in order to assist with the investigation of a complaint.

Reliability of email - Users should bear in mind that the e-mail system cannot guarantee that received messages have been sent by the claimed sender and have not been modified en-route.

3.1.3.3 Access control

Default Privileges—Electronic communication systems must be established and maintained such that only the privileges necessary to perform a job are granted to a user. For example, when a users relationship with ECDC comes to an end, all of the users privileges on ECDC electronic communications systems also must cease. With the exception of emergencies and regular system maintenance notices, broadcast facilities must be used only after the permission of head of ICT has been obtained.

User Separation—Where electronic communications systems provide the ability to separate the activities of different users, these facilities must be implemented. For example, electronic mail systems must employ personal user IDs and secret passwords to isolate the communications of different users. Unless a computerized fax mailbox system is employed, fax machines that do not generally have separate mailboxes for different recipients, so such user separation is not required. If ECDC has established user separation, users must not employ the user ID or the identifier of any other user.

User Identity—Misrepresenting, obscuring, suppressing, or replacing another user's identity on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings. With the exception of helpdesk service that is intended to be anonymous, users must not send anonymous electronic

communications. At a minimum, all users must provide their name and phone number in all electronic communications. Electronic mail signatures indicating job title, organization affiliation, address, and other particulars are strongly recommended for all electronic mail messages. Digital certificates are also recommended for electronic mail as a way to authenticate the sender's identity.

3.1.3.4 Use of Encryption

Use Of Encryption Programs—Users are reminded that ECDC electronic communications systems are not encrypted by default. If sensitive information (classified as Confidential or Secret) must be sent by electronic communication systems, an encryption process approved provided by ECDC ICT must be employed. Mobile computers, notebook computers, portable computers, personal digital assistants, and similar computers that store ECDC sensitive information must consistently employ disk encryption provided by ECDC ICT to protect this sensitive information when it is stored inside these same computers, and when it is stored on accompanying data storage media. Users of these types of computers who are recipients of sensitive information sent by electronic mail must delete this information from their systems if they do not have encryption software that can properly protect it. Separately, users must not use encryption for any production electronic communications system unless the solution has been deployed by ECDC.

3.1.3.5 Exceptions on Privacy

No Guaranteed Message Privacy—ECDC cannot guarantee that electronic communications will be private. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Electronic communications can be accessed by people other than the intended recipients in accordance with this policy. Because messages can be stored in backups, electronic communications actually may be retrievable when a traditional paper letter would have been discarded or destroyed. Users must accordingly be careful about the topics covered in ECDC electronic communications, and should not send a message discussing anything that they would not be comfortable reading about on the front page of their local newspaper.

Statistical Data—As outlined in 2.3 and in respect to [3,4,5], ECDC collects statistical data about its electronic communication systems. For example, call detail reporting information collected by telephone switching systems records the numbers dialed, the duration of calls, the time of day when calls were placed, etc. Using such information, technical support personnel monitor the use of electronic communications to ensure the ongoing availability, reliability, and security of these systems. EDCD will employ computer systems that analyze these types of statistical information to detect unauthorized usage, toll fraud, denial of service attacks, and other problems.

4 Annex

4.1 Reference

[1] Staff regulations of the EC

[2] NOTE AUX MEMBRES DE LA COMMISSION: Information relative à un arrêt du Tribunal de Première Instance prononcé le 19 mars 1998, SERVICE JURIDIQUE, 20 mars 1998.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[4] **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)**.

[5] Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data

4.2 Individual Declaration

Individual Declaration on the Use of Computer Systems and Services Supplied by ECDC

I have read and familiarized myself with the terms and conditions of use of the ICT systems and services supplied by the ECDC. I will use those systems and services responsibly and I undertake to comply with the principles defined in the ECDC ICT use policy.

I understand that in the event of misuse of information systems or services, penalties and other measures may be applied in accordance with my contract with ECDC.

Name: Date:

Signature:

Use of any computer system or service supplied by ECDC shall be taken as signifying acceptance of this declaration

4.3 Guidelines for constructing good passwords

Choosing and using passwords requires some care in order to ensure that it will be difficult for attackers to guess or find out the password.

A good password must not contain:

- the user login name;
- the user name or user's nickname;
- names of user's friends or relatives;
- information that is associated with the user and is widely available, for example telephone numbers, date of births, vehicle registration number, home address, etc;
- repetition of a small number of characters, for example *pppLLL3* or *pLpLpL3*;
- words that are listed in dictionaries of any language.

Passwords must have at least eight (8) alphanumeric characters and must contain characters from at least three of the following four classes:

- English Upper Case Letters (A, B, C, ... Z)
- English Lower Case Letters (a,b,c, ... z)
- Numeric Characters (0,1,2, ... 9)
- Special Characters (;:*%!...)

Ideally, a password should consist of a combination of mixed-case alphabetic, numeric and punctuation characters, for example: *fiwRQ7S+*.

A password must be easy to remember so that the user does not have to write it down in order to remember it. In addition, passwords must be easy to type. This would reduce the time the user needs to type it and thus reduce the possibility that someone can steal the password.

One efficient and secure way to derive easy-to-remember passwords is to choose a song or any other piece of favourite text and use the first character of each word. The result can then be combined with some digits and/or punctuation characters. For example the phrase "To be or not to be" produces the character sequence T*borntb*, which can then be combined with the punctuation characters *;!* to get the password *Tborntb;!*.

Finally, users should change their passwords but they must not choose passwords that are similar to or can be easily derived from previous passwords. In particular, users must not construct passwords by concatenating a static set of characters with a set of characters that changes in a predictable way. An example of an inappropriate password series is <"*zdthm.01*", "*zdthm.02*", "*zdthm.03*"... >. Although each one of these passwords is a proper password, the fact that the passwords change in a predictable way renders the password series inappropriate.