

ANNEX

IT PROCEDURES

1. IT infrastructure	2
2. Files organisation (network)	9
3. IT Responsibilities	14
4. Security	16
Responsibility and authority	16
Retention Schedule	14
Physical security	17
Hardware Security	18
Network security	18
Software security	18
Communication security (emails)	19
Data security	19
Media handling and security	20
Security measures in case of disaster	20
Confidentiality statement	22
5. Software applications	23
6. Backups	25
General	25
CONTAB	25
Perseus	28
WebRamis	28
Media	28
Project Documentation	28
User Data	28
7. Training	25
8. Forms	25

1. IT infrastructure

The CFCU is located 44, Mircea Voda Blvd, Entrance B, Sector 3, Bucharest.

In the CFCU there are around 81 workstations and 5 servers connected in a Local Area Network (LAN). The main operating systems are Microsoft based. There are various network servers (5) for different purposes. These servers are all located in one room.

CFCU is connected to the Internet through a private Internet provider, Datek Telecom. The contact data of the persons responsible for the Internet are setout below:

Name	Function	Email	Phone
Alin Radulescu	Sales representative	alin.radulescu@datek.ro	021 312 0401

An inventory list of hardware, users and location is kept at the administration. This list, Annex No. 2 is updated on a regular basis by the Administrator.

A list of the main CFCU IT equipment (non-relevant equipment as telephones, flash sticks, network components as UTP cable, outlets, switches etc are not mentioned here) is specified below:

Nr	Items	Quantity
1	Main Server	1
2	Workstations type I	5
3	Workstations type II	61
4	Workstations type III	15
5	UPS	66
6	Notebook	5
7	Mobile back-up solution	1
8	External hard disk drive	1
9	Digital Copier - type I	2
10	Digital Copier - type II	1
11	Color printer	1
12	Network printer - type I	4
13	Network printer - type II	2
14	Professional scanner	1
15	Scanner	2

16	Fax machine	2
17	Mobile audio recording system	3
18	Acrobat Writer or equivalent	10
19	Adobe Photoshop or equivalent	10

1. Main Server

Processor 2xIntel Xeon, minimum 2.4GHz Hyper-Threading 533 MHz FSB Hyper Threading or equivalent
 Server System Infrastructure Chassis 2x400W redundant
 Memory 1GB RAM (max. 8GB ECC registered)
 HDD: Storage capacity RAID 1 mirroring 2x120GB buffer 8MB
 Display Card with Video 32Mb RAM
 Network card 10/100 & 10/100/1000 Server LAN
 3.5" 1.44 MB Floppy Drive
 CD-RW/ DVD Combo Box drive, minimum speeds: DVD 16x read; CD-RW 52x/52x/32x read/write/re-write
 17" Flat Display, minimum 0.25dpi, 1280x1024@75Hz
 104 keys Multimedia Keyboard in accordance with US ASCII standard
 Optical Mouse, Intellimouse compatible, 3 buttons, scroll
 Hardware Monitoring
 OS Linux, including updates for three years
 3 years warranty
 UPS: Runtime at least 30 minutes typical backup time at half load / 10 minutes at full load, Output power capacity minimum 2000 VA, Management software (incl. shutdown facility)
 Antivirus software for E-Mail Sever – includes installation, configuration for each mail box, updates for three years (note: BitDefender was delivered)
 OS installation, Server configuration: DHCP, DNS, E-Mail Server
 3 years warranty

2. Workstations type I

Pentium IV 3.2GHz or equivalent
 Motherboard 800MHz FSB, Dual DDR/400MHz, AGP 8x, S-ATA, PCI, USB 2.0, ATA100, audio
 ATA100, Serial ATA, PCI, USB 2.0, RAID, audio
 120GB Hard Disk 8MB buffer
 2x512MB Dual DDRAM 400MHz PC3200
 Display Card with Video 256MB DDRAM, TV out, AGP 8x
 Network card 10/100Mb
 3.5" 1.44 MB Floppy Drive
 DVD-RW (DVD+R, DVD-R) drive DVD/CD-ROM reading speed: 12x/40x; DVD writing/rewriting speed: DVD+R/RW 8x/4x; DVD-R/RW 4x/2x; CD-R/RW writing/rewriting speed: 24x/10x
 104 keys Multimedia Keyboard in accordance with US ASCII standard
 Speakers 2x20W
 Optical mouse, Intellimouse compatible, 3buttons, scroll
 Ports: 1 serial, 1 parallel, 2 USB

Middle tower
19" TFT Display, contrast minimum 600:1, maximum 0.25dpi, 1280x1024@75Hz
OS Windows XP Professional OEM
Microsoft Office XP Professional Retail
Antivirus Software, incl. license and updates for three years (note: BitDefender was delivered)
3 years warranty

3. Workstations type II

Pentium IV 2.8GHz or equivalent
Motherboard 800MHz FSB, Dual DDR/400MHz, AGP 8x, PCI, USB 2.0
ATA100, Serial ATA, audio
80GB Hard Disk 8MB buffer
2x512MB Dual DDRAM 400MHz PC3200
Display Card with Video 128MB DDRAM, TV out, AGP 8x
Network card 10/100Mb
3.5" 1.44 MB Floppy Drive
combo CD-RW/DVD-ROM drive, minimum speeds: DVD 16x read; CD-RW 52x/52x/32x read/write/re-write
104 keys Multimedia Keyboard in accordance with US ASCII standard
Speakers 2x15W
Optical mouse, Intellimouse compatible, 3buttons, scroll
Ports: 1 serial, 1 parallel, 2 USB
Middle tower

17" Flat Display, maximum 0.25dpi, 1280x1024@75Hz
OS Windows XP Professional OEM
Microsoft Office XP Professional Retail
Antivirus Software, including license and updates for three years (note: BitDefender was delivered)
3 years warranty

4. Workstations type III

Pentium IV 3.0GHz or equivalent
Motherboard 800MHz FSB, Dual DDR/400MHz, AGP 8x, PCI, USB 2.0
ATA100, Serial ATA, audio
70GB Hard Disk 8MB buffer
512MB DDRAM 400MHz PC3200
Display Card with Video 128MB DDRAM, TV out, AGP 8x
Network card 10/100Mb
3.5" 1.44 MB Floppy Drive
combo CD-RW/DVD-ROM drive, minimum speeds: DVD 16x read; CD-RW 52x/52x/32x read/write/re-write
104 keys Multimedia Keyboard in accordance with US ASCII standard
Speakers 2x15W
Optical mouse, Intellimouse compatible, 3buttons, scroll
Ports: 1 serial, 1 parallel, 2 USB

Middle tower
17" Flat Display, maximum 0.25dpi, 1280x1024@75Hz
OS Windows XP Professional OEM
Microsoft Office XP Professional Retail

Antivirus Software, including license and updates for three years (note: BitDefender was delivered)
3 years warranty.

5. UPS

To support 1 computer and 1 monitor
Minimum 10 minutes autonomy
Management software (incl. shutdown facility)
3 years warranty

6. Notebook

Pentium IV, minimum 2.8GHz or equivalent
60GB, 7200rpm Hard Disk
512MB DDRAM
Display Card with Video 64Mb RAM, SVGA, TV out
On board audio, network card 10/100 and modem 56Kbps (V90), V,92 ready
Interfaces: DC-in, external microphone, external monitor, headphone (stereo), parallel, RJ-11, RJ-45, TV-out (s-video), USB 2.0
Built-in speakers
3.5" 1.44 MB Floppy Drive
DVD-R/RW drive, maximum speed: Read: 24x CD-ROM, 16x CD-R, 10x CD-RW, 8x DVDROM,
4x DVD-R, 4x DVD-RW / Write: 16x CD-R, 10x CD-RW, 1x DVD-R, 1x DVD-RW
Optical mouse, Intellimouse compatible, 3 buttons
15" TFT
Ports: 1 serial, 1 parallel, 2 USB, PCMCIA
Carry case
OS Windows XP Professional OEM
Microsoft Office XP Professional Retail
Antivirus Software, including license and updates for 3 years (note: BitDefender was delivered)
1 year warranty

7. Mobile back-up solution

The solution must provide comprehensive cross-platform backup/recovery, disaster recovery, data replication, and hierarchical storage management. Shall be compatible with the existing IBM Server (HDD 97.5 GB, Pentium III 1.1GHz, 256 MB RAM, CD-ROM 52x, Windows 2000 Server)
Backup Software to ensure complete data protection across business-critical applications such as messaging / groupware, databases and files
must include mobile rack system for removable storage devices that will be used secondary to the local backup system, to prevent disaster
minimum capacity 250 GB
Installation and configuration
3 years warranty

8. External hard disk drive

External hard disk, at least 250GB capacity, 7200rpm, 8MB buffer size
compatible with the mobile back-up solution
interface: USB 2.0

3 years warranty

9. Digital Copier type I

Black and white copier, digital copying technology

A3 format

Copying speed: minimum 60ppm A4

Duty cycle: 150,000 copies per month

Automatic document feeder

Paper capacity: minimum 5,000 sheets

Paper sources: minimum 3

Two-sides copying (duplex copying)

Sorter: minimum 20 separate output bins

Stapler

Include consumables for 2 duty cycles

3 years warranty

10. Digital Copier type II

Black and white copier, digital copying technology

A3 format

Copying speed: minimum 30ppm A4

Duty cycle 80,000 pages per month

Automatic document feeder (ADF)

Paper capacity: minimum 1,500 sheets

Paper sources: minimum 2

Sorter: minimum 20 separate output bins

Include consumables for 2 duty cycles

3 years warranty

11. Color printer

Color Laser technology

Format: A3

Processor: minimum 500MHz

RAM: minimum 96MB

Printing resolution: minimum 1200x1200dpi

Printing speed: 20ppm B&W and 20ppm full color (A4)

Network card 10/100 Base-TX

Paper trays: minimum 2 (A4, A3)

Print-server for the important OS, including drivers

Consumables: for 30,000 copies

3 years warranty

12. Network printer type I

Laser technology, black & white printing

Format: A3

Network connectivity 10/100Base-TX

RAM: minimum 64MB (expandable)

Duty cycle at least 100,000 pages/month

Automatic duplex printing

Printing speed: minimum 50ppm A4

Resolution: minimum 1200x1200dpi

Include consumables for 2 duty cycles
3 years warranty

13. Network printer type II

Laser technology, black & white printing
Format: A3
Network connectivity 10/100Base-TX
RAM: minimum 16MB (expandable)
Duty cycle at least 80,000 pages/month
Printing speed: minimum 30ppm A4
Resolution: minimum 600x600dpi
Include consumables for 2 duty cycles
3 years warranty

14. Professional scanner

Color scanner
Originals size:A3
Minimum 2400x2400dpi optical resolution, true 48-bit colour
Duplex ADF (Automatic Document Feeder)
Associated drivers and software (OCR software included)
USB 2.0 connectivity
3 years warranty

15. Scanner

Color scanner
Originals size: A4
Minimum 2400x2400dpi optical resolution, true 48-bit
USB 2.0 connectivity
Associated drivers and software (OCR software included)
3 years warranty

16. Fax machine

Laser Fax Machine
36.6kbps High speed Fax Modem
Interfaces: USB, Parallel, PC
Print speed : at least 15ppm
100 telephone numbers memory
Multiple transmission function (single scan, multiple locations transmission)
Telephone function (handset included)
2 years warranty

17. Mobile audio recording system

Recording capacity: 600 hours
Data format: PCM or MP3
Ethernet interface for PC/network connectivity
Inputs for microphones: 6
The system should allow for storage of the recorded material on removable media (preferable CD or DVD)
The system shall be used in different tendering rooms, therefore it shall be easily movable.
Includes: cables, microphones, microphone mixer, software, installation

3 years warranty

Remarks

- The e-mail and back-up servers are not effectively used (although installed). The e-mail server is stored at the CFCU Internet Service Provider (which assures also anti-spam and antivirus scanning) and the back-up server is configured to back-up only the e-mail server (which is not used at this moment).

Beside the equipment listed here below, there is some supplementary equipment:

- additional computers (same type as position "3. Workstation type II")
- computers received through the Phare supply project related to SMIS
- one old server running Windows NT 4, which is still used as primary domain controller (incl. management of users and registration of network printers), gateway for the Internet connection and file server
- one old (but much better than the previous one) IBM server running Windows 2000 server (practically not used; there is no intention to move here the functionalities of the poorer above mentioned server)
- one old server used for accounting software and WebRAMIS (both use Oracle databases)
- one old workstation where Perseus is installed (the CFCU waits some help from Brussels to move Perseus to one of the new workstations)
- there are some problems with the licenses for the Windows NT and 2000 servers as it seems that the CFCU does not have user extensions for all the new users.

Procedures for protection against environmental factors

- In terms of facilities, central computing resources are located on a floor capable of solid construction with appropriately secured entry.
- The areas used for central servers and communications equipment have appropriate environment controls that include temperature and humidity.
- A strict 'No Smoking' policy is observed in all computing facilities.
- All key computing equipments are maintained in accordance with the supplier's recommended service intervals and specifications.
- Alarm and intruder detection systems are installed.
- The rooms have air conditioning.
- A safety measure for protection against fire is the fire extinguishers that are located in every room.

2. Files organisation (network)

Having in view the types of documents used in electronic format, the following structure of directories has been setup for organising the documents on the server:

<i>Directories</i>	<i>Explanations</i>
Programmes	It contains documents related to the programme as a whole (not related to a certain project within the programme), organised by sub-directories as follows:
N_{ix} <Phare or ISPA programme>	There should be one directory for each Phare or ISPA programme. The name of the directory should be the short identification of that programme (eg. Phare2000, Phare2001, ISPA2000 etc.). Each directory should contain documents directly related to that programme, organised by sub-directories as follows:
Financing memorandum	financing memorandum, annexes, addenda to financing memorandum etc.
Reports	reports related to the implementation of the programme
Financial	financial documents related to the programme
Templates	various standard templates
Manuals	relevant manuals (eg. manuals of procedures)
Common documents	It contains documents that are of common interest of the whole institution and that are not related to a certain project or programme.
Departments	It contains documents for the internal use of only one department, organised by sub-directories as follows:
Administration	administrative documents for the use of directors and/or secretaries

<i>Directories</i>	<i>Explanations</i>
⊢ $N_2 x$ <top level department>	There should be one directory for each top level department. Each directory should contain documents for the internal use of only that department.
└ Users	It contains documents that are managed by only one person.
⊢ $N_3 x$ <user's name>	There should be one sub-directory for each user. The name of the directory should be the name of that person. Each directory should contain documents that are managed by that person , organised by sub-directories as follows:
⊢ Confidential	It contains confidential documents that should not be read by anybody else than the person that manages these documents. Note: The documents should be stored in this directory only temporary. When a document is no longer confidential, then it should be moved to one of the open directories, as appropriate.
⊢ $N_{4i} x$ <code of project>, $i=1..N_3$	There should be one sub-directory for each project managed by that person. The name of the directory should be the code of the project. Note: Here, by “project” is meant either projects or sub-projects, depending which of them is the bottom level in the hierarchy. If a project contains sub-projects, then these sub-projects should be treated as they would be some individual projects. Each directory should contain documents directly related to that project, organised by sub-directories as follows:
⊢ Contracting preparation	contract forecast, procurement notice, Terms of Reference / Technical Specifications etc.

Name of procedure: IT Procedure

<i>Directories</i>	<i>Explanations</i>
┆ Shortlisting	establishment of the shortlist panel, shortlist report and other related documents, notifications, shortlist notice etc. Note: This is an open directory (it may be read by other staff members). The documents that are confidential should be stored in the “Confidential” directory of the user that manages those documents, until they are no longer confidential and then they may be moved here.
┆ Tendering	tender dossier, invitations, establishment of the evaluation committee, evaluation report and other related documents, notifications, contract award notice etc. Note: If more tenders are organized for the same project, then more directories of this type could be added here and their names could be appended by appropriate numbers (eg. “Tendering1”, “Tendering2” etc.). Note: This is an open directory (it may be read by other staff members). The documents that are confidential should be stored in the “Confidential” directory of the user that manages those documents, until they are no longer confidential and then they may be moved here.
┆ Contract	contract dossier, addenda etc.
┆ Reports	reports related to the implementation of the project
┆ Financial	financial documents related to the project

Any sub-directory may be added within any of the directories (especially within the bottom level directories) in order to adjust the structure to the practical needs.

The following groups of users should be set in order to allow an easier control of access rights for these directories:

- N x <department> – There should be one group for each bottom level department or sub-department. Each group contains all users in that department.
- Directors – the director and the deputy directors;
- Secretariat – the secretaries;

Name of procedure: IT Procedure

- IT Administrators – users designated as IT administrators;
- All Users – all users of the staff of CFCU.

The following access rights should be set for each of the directories:

<i>Directories</i>	<i>Owner of directory</i>	<i>Groups to be awarded the read right</i>	<i>Groups to be awarded the write right</i>
Programmes	OS administrator	All Users	All Users, except for Secretariat
Templates	OS administrator	All Users	IT Administrators
Manuals	OS administrator	All Users	IT Administrators
Common documents	OS administrator	All Users	All Users
Departments	OS administrator	All Users	IT Administrators
Administration	OS administrator	Directors, Secretariat	Directors, Secretariat
$N_2 x$ <top level department>	OS administrator	$N_{5j} x$ <sub-department belonging to department j >, $j=1..N_2$	$N_{5j} x$ <sub-department belonging to department j >, $j=1..N_2$
└ Users	OS administrator	All Users	IT Administrators
$N_3 x$ <user's name>	<user i >, $i=1..N_3$	All Users	IT Administrators
Confidential	<user i >, $i=1..N_3$	Directors	-
$N_{4i} x$ <code of project>, $i=1..N_3$	<user i >, $i=1..N_3$	All Users	-

Notes:

- By default, the sub-directories and the files have to be set with the same access rights as their parent directory.
- The owner of a directory or file has full access rights on that directory or file.

PS 049	Edition: C.	Date: 15.12.2005	Page 12 of 29
--------	-------------	------------------	---------------

- The administrators of the server have full access to all directories and files.

When a user is temporarily missing, then another user should be granted full access rights on the sub-directory (and its entire content) of the missing user, within the “Users” directory. These access rights have to be revoked as soon as the owner of the sub-directory returns to work. When a user is no longer working for the institution, then the documents that are still under work have to be copied to the sub-directories of other users, according to the repartition of tasks decided by the appropriate Head of Department or Director. The directory of the former user must be kept.

3. IT Responsibilities

Responsibilities of the Information Technology Department

The IT Team (ITT) is responsible for the efficient use of information systems and communication measures, such as electronic mail, in the CFCU to enable users to achieve the goals and objectives of the organization.

IT functions/systems	Person(s) responsible
Network administrator	Mr Gabriel Varnaiote Mr Constantin Saragea (backup)
DRMS	Mr Gabriel Varnaiote Mr Constantin Saragea (backup)
CONTAB	Mrs Ludita Chiricuta Mrs Monica Manolea
RAMIS	Mrs Madeleine Tolea Mrs Anamaria Marinescu
PERSEUS	Mrs Malalina Ilie
SMIS	Mrs Madeleine Tolea Mrs Madalina Ilie

The main responsibilities are the following:

- Developing and advising CFCU on its information technology investment strategy.
- Procurement of new computer hardware, software and networking
- Availability of IT infrastructure
- Installation and maintenance of hardware and networks
- Installation of software
- Installation of a mail client tool
- Installation of the organization approved anti-virus software
- Installation of the necessary applications – Microsoft Office 2003, Professional Romanian, Contab or Perseus.
- Set up the access to Internet
- Ensure the necessary IT equipment is in place
- User account management (creation, and up keeping of user accounts and passwords).
- Troubleshooting to solve problems
- Ensuring security of data by:
 - Carrying out backup and restore procedures.
 - Training of (new) computer users including training on:
- CFCU anti-virus policy
- Backup policy
- Security responsibility.

Establishment of centralized management system of user rights.

- The Administrator develops user domain accounts, which optimizes IT resources allocated for the CFCU staff and ensures security of hardware, software and data;

- The Administrator assigns login names to the CFCU staff;
- User access rights are reviewed at 6 months intervals using Annex no 1;
- All CFCU staff construct “strong” passwords and use them in a secure manner;
- All CFCU staff enter login names and passwords to use CFCU computer resources;
- The Administrator ensures that:
 - in the absence of a staff member for 5 minutes or more, screensaver appears, which can be switched off by re-entering login name and password;
 - all system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) are changed on at least a quarterly basis;
 - all system-level passwords are administered and controlled by the ITT staff in a secure manner;
 - all user-level passwords are changed at least every three months;
 - users who have more than one account on a system to allow different levels of access have a unique password for each account;
 - the password have 8 digits, from which minimum 2 must be figures.

When a new person is hired, the Director of his/her Department should inform the LAN Administrator in order to create an email account and a domain account for the new employee, using Request No.1.

When a person leaves the institution or he /she has been suspended from the CFCU, the Director of his/her Department should inform the LAN Administrator. The Administrator will delete the person-related accounts.

Security-related reporting

CFCU staff reports security-related events to the ITT staff, who will review logs and report incidents to the Director where appropriate. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- port-scan attacks;
- evidence of unauthorized access to privileged accounts;
- anomalous occurrences that are not related to specific applications on the host;

According to the type of problem/request, the LAN Administrator will decide whether he can deal with it or contact the relevant IT firm that provided the problematic equipment or contact ITT.

4. Security

Responsibility and authority

Security Team

The CFCU needs a high level of IT security, given the confidential nature of its activities. The security team is headed by the Organisation Security Officer (OSO).

The security team (comprised of 2 members) is internal to the CFCU and is empowered to effectively define security standards and implement security policies in close cooperation with ITT.

The OSO is in charge of the security team. The OSO is responsible for articulating the overall shared vision that will be used to develop the organization security policy and define the work of all other security team members.

The OSO has the following major responsibilities:

- Recommend security strategies.
- Ensure that information security policies and procedures are established and implemented to protect the information assets of the CFCU.
- Participate in the creation and review of these policies and procedures.
- Keep information security systems current.
- Update accordingly the security procedures.
- Ensure that the security model is communicated to the highest levels within the organization and that the security plan has a sponsorship commitment at the appropriate senior executive level.
- Be part of the decision-making team when the organization is designing, planning, procuring or upgrading technologies.
- Be the single point of contact for all issues involving information security including, but not limited to, questions, alerts, viruses, and breaches.
- Inform the executive management of breaches, information security activity, and risks.

Retention Schedule

A Retention Schedule is a control document that sets out the periods for which an organisation's business records should be retained to meet its operational needs and to comply with legal and other requirements.

A Retention Schedule is an essential component of an efficient and effective records management system. Properly developed and consistently implemented, a Retention Schedule protects the interests of the organisation and its stakeholders by ensuring that business records are kept for as long as they are needed to meet operational needs and to comply with legal requirements, and are then disposed of securely.

Internet Acceptable Use Policy

This Acceptable Use Policy (AUP) applies to all CFCU staff to using the IT resources. For the purposes of this document the 'internet' is defined as: web applications (WebRamis, PERSEUS, SMIS and DRMS), e-mail, web services,

<http://europa.eu.int/comm/europeaid/cgi/frame12.pl>. This policy should be considered part of the Conditions of Use for Computers and Networks at CFCU.

Use of Internet is monitored for security and/network management reasons. Users may also be subject to limitations on their use of such resources.

Unacceptable Use or behaviour:

It is unacceptable to:

- Visit Internet sites that contain obscene, hateful or other objectionable materials.
- Make or post indecent remarks, proposals or materials on the Internet including racist or sexist jokes and defamatory comments.
- Upload, download or otherwise transmit commercial software or any copyrighted materials belonging to parties outside of the CFCU, or the institution itself unless this download is covered or permitted under a commercial agreement or other such licence.
- Download any software or electronic files without implementing virus protection measures that have been approved by the CFCU
- Intentionally interfere with the normal operation of the network, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders others in their use of the network
- Monitor Network Traffic Content or scan devices connected to the network.

Users should:

- If you become aware that there has been unauthorised access to your computer, you must raise it immediately with the IT Team because of the implications for the security of CFCU, and personal data.
- Record any instances where you have accessed inappropriate sites by accident. For example this may be through mistyping an address or spam email link.
- Log out of the computer when you have finished Monitoring

Information is the lifeblood of any organisation and it is vitally important that we protect the confidential information that we hold, maintain the integrity and ensure availability.

Physical security

- IT equipment is distributed to the personnel and it is located in rooms with limited access. The doors are locked at the end of day and only the authorized personnel have access.
- All the servers are located in a secured locked room. The room is locked all the time unless there is a need to conduct certain technical work.
- All power and telecommunications lines into computing facilities are enclosed and secured.
- The rooms have air conditioning and fire extinguisher.
- Access to the organization is based on identity cards. The organization has 24 hour security guards.
- Access to the servers rooms is restricted to authorized personnel, IT Team only;
- Visitors are accompanied during their visit to the organization.
- Personnel who have left the institution or have been suspended are not allowed to enter the CFCU.

- At the end of each working day, the rooms are locked and only authorized personnel are permitted to have access to the keys.
- The Administrator registers all visitors to the server facilities; information about visitors is kept for at least two years.
- It is forbidden to smoke in rooms with IT equipment.

Hardware Security

Administration of Hardware security

- The responsibility for administration of hardware security depends on the equipment and it is distributed as follows:
 - Each user is responsible for his/her workstation.
 - The Network Administrator is responsible for all the IT equipment stored in the servers' room.

Hardware maintenance

- Every workstation owned by CFCU is tagged.
- All key computing equipment is maintained in accordance with the supplier's recommended service intervals and specifications.
- Only authorized maintenance personnel are permitted to carry out repairs and service equipment.
- If a member of staff requires some additional IT equipment or software he will use the Request No. 3, then appropriate procurement procedures must be followed. The IT Team check the new software using a separately workstation situated in the servers room. After that the IT Team decided if the new software is technical compliant with the requirements.
- A list of suspected or/and actual faults to the equipment is kept by the LAN Administrator.
- All staff uses a Request No. 4 for notification to solve the computer mal function.

Network security

- All Network Cabling is installed and tested by qualified and authorised personnel only.
- Network cabling at hubs, switches, routers, etc are appropriately identified and kept tidy using cable ties, suitable lengths of 'patch' cables, etc.

Software security

- Personnel are not allowed to install any application software on their own.
- If a member of staff requires some additional software then appropriate procurement procedures must be followed.
- The Administrator ensures that the standard, supported anti-virus software (BitDefender) is running on every computer used within the CFCU. The windows updates are automatically installed on the workstations.
- The staff is not allowed to disable or remove the virus protection software (BitDefender) or any other software from any computer.
- The staff does not change the settings for emails account and network connection.
- Only the Administrator disables the unused software.

- The Administrator takes all available measures to rule out unauthorized downloading of application software.
- All users are required to comply with copyright and software licensing agreements.
- Uploading and downloading copyright protected material is expressly prohibited. Displaying or posting copyrighted material on any Intranet or Internet server (servers placed in the perimeter network) is expressly prohibited.
- Personnel do not have rights to share information on their workstations.

Communication security (emails)

Administration of communication and Security characteristics

- Internal and external communication is based on the telephone exchange, the email and website.
- The Administrator is responsible for creating and maintaining the email accounts, but each employee is responsible for his/her email
- Personnel must:
 - not disable or remove virus protection software from any computer.
 - never open any files or macros attached to an email from an unknown, suspicious or untrustedworthy source and delete these attachments immediately, then “double delete” by emptying their recycle bin.
 - not use the electronic mail services for: unlawful activities; commercial purposes not under the auspices of the Ministry; personal financial gain; or purposes that contravene other Ministry policies or guidelines. The latter include, but are not limited to, policies regarding: sexual or other forms of harassment, religious or political activities or copyright.
 - when creating and sending email, users of electronic mail services should take care not to give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the Ministry or any unit of the Ministry unless appropriately authorised (explicitly or implicitly) to do so.
- The Administrator is responsible for the email server and the email accounts maintenance.

Protection of information in communication environment

- The anti-virus software is installed on every workstation.
- The Bit Defender software is automatically update on regular basis- from every 3 hours to every 24 hours;
- If an email contains viruses, it will be automatically deleted from the server.
- The Mail Server is backed up appropriately and controls are in place to prevent unauthorized staff gaining access to other people’s emails.

Data security

- The Administrator is responsible for data and information security.
- Each employee is responsible for the local data from his/her computer.
- In the absence of a staff member for more than 5 minutes, screensaver appears, which can be switched off by re-entering the user name and password;
- Every email account has a user name and password and only the owner of the account knows the password. In addition, the personnel must deliver the user-level passwords

in a sealed envelop to the Administrator. Authorized personnel have the right to open the envelopes in case of emergency.

- All system-level passwords e.g. root, NT admin, application administration are changed on at least a quarterly basis;
- All system-level passwords are administered and controlled by the Administrator from the CFCU building in a secure manner;
- All user-level passwords are changed at least every three months or when the passwords are compromised;
- No equipment, documentation or data may be taken off-site without the appropriate authorisation.
- There is anti-virus installed on the server and on every work station within CFCU.
- Hard copy data of no longer use is destroyed. Hard copy data referring here to letters (draft and final versions), tender documentation, project documents, reports that might contain data that is considered confidential.
 - Before destroying it is kept in a secure environment with limited access.
 - While destroying the process includes measurements to ensure that data is destroyed properly before it is purged, using the Request No. 2.

Media handling and security

- All CDs are kept in a secured locker. Only the Administrator has access to this locker therefore he is responsible for the security of the media.
- When an employee needs a CD, (s)he has to contact the Administrator because he is the only one authorized to install software on the workstations.
- The room has air conditioning and fire extinguisher.
- The documentation is stored in a secured, lockable fireproof safe or cabinet for each department within the CFCU.
- Software CDs are backed up.
- No equipment, documentation or data may be taken off-site without the appropriate authorisation.

Security measures in case of disaster

The main objective of a Disaster Recovery Plan is to enable the organisation to survive a disaster and to re-establish normal business operations.

To elaborate a good plan, the potential sources of disaster must be identified:

Objects to be recovered	Potential sources of disaster					Priority
	Electronic Security	Hardware Failure	Fire	Power Outages	Physical security (Flood/ Storm/ Sabotage)	
Database	X	X	X	X	X	1

Media (software from other organizations)	-	-	X	-	X	4
Project documentation	-	-	X	-	X	1
User Data	X	X	X	X	X	2
Servers	X	X	X	X	X	1
IT Equipment			X	X	X	3

*Legend 1 is High Priority
5 is Low Priority*

Roles and Responsibilities

Actions	Responsible
Administration and Maintenance of IT equipment.	IT Team
Media and Documentation	Administrator, Directors of Departments
Databases	Administrator

The detailed procedures are described in the *Section 6. Backups*

Disaster Recovery Plan - testing and updating

Plan testing is a critical element of a viable disaster recovery capability. Testing enables plan deficiencies to be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Each element should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. The following areas should be addressed in a contingency test:

- System recovery on an alternate platform from backup media
- Internal and external connectivity
- System performance using alternate equipment
- Restoration of normal operations

Plan maintenance

To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies. Electronic Information Resources undergo frequent changes because of changing business needs, technology upgrades, or new internal or external policies. Therefore, it is essential that the plan be reviewed and updated regularly, as part of the CFCU's change management process, to ensure new information is documented and contingency measures are revised if required.

As a general rule, the plan should be reviewed for accuracy and completeness at least annually or whenever significant changes occur to any element of the plan. Certain elements will require more frequent reviews, such as contact lists.

Confidentiality statement

All users of the information system are required to take necessary precautions to protect the confidentiality of data encountered in the performance of their duties. In this respect, confidentiality statements are signed by the CFCU employees.

The violations of CFCU policies may result according to the confidentiality statement, in various disciplinary actions up to dismissal.

5. Software applications

MS Office standard software applications are used for text processing, calculation spreadsheets, presentations etc. In addition some special software tools are used for various purposes, such as accounting. These software applications have been provided by external sources such as the EU commission, or have been developed by contracted private partners.

Software	Technical Specification
Document Registration and Monitoring System (DRMS)	Web application Database: postgreSQL Programming Language: php
WebRAMIS	Oracle
CONTAB	Oracle
PERSEUS	Microsoft Access
SMIS	Oracle

The persons indicated in chapter 3 (IT responsibilities) are responsible for the installation of the corresponding software applications on the workstations and the servers.

The backup and restore procedures for the previous mentioned software are described in details in the **Section 6. Backups**

Document Registration and Monitoring System (DRMS)

The main use of this software is to enable the users to register and keep track of the incoming and outgoing documents within CFCU.

A user manual is available for the CFCU personnel.

Perseus

The PERSEUS application is a reporting tool to support reporting to the European Commission in Brussels about the EU programme funding, contracting and disbursements. The application is stand-alone and it is installed on one computer, located in the Department of Financial Reporting.

A user manual is available for the CFCU personnel in the “PERSEUS Procedures” (PH 05 – PS 512 attach 1).

WebRamis

This application supports technical and financial reporting for ISPA programme. A special function within the application enables the users to take over data from the CONTAB application.

A user manual is available for the CFCU personnel.

Contab

Contab is the accounting application used for ISPA and recently for Phare programme as well. It permits the taking over of the data by the WebRamis reporting system.

A user manual is available for the CFCU personnel in the “Computer Based System” procedures (PH07 – PS 734 attach 1).

SMIS

The application is destined to cover the whole necessary information related to all projects financed by the European Commission in Romania. It shall have two modules: one for the pre adhesion programs and one for the post adhesion programs. The application is still under development and a first release is available for testing purpose.

A user manual will be available for the CFCU personnel.

6. Backups

General

- At the CFCU headquarters a dedicated data server is running and available all times to store and make weekly backups for all users data;
- This dedicated data server is UPS protected in order to avoid loss of data due to power failure;
- This server has enough disk space for restoring the entire information stored from the backup media, that it is equipped with a media drive compatible with the drives on the users PC's;
- the media drive on the data server is tested regularly by the Administrator (a simple .txt file copied from removable media on the server's hard disk and then opened with Notepad application) and kept in working conditions;

- All key data are classified in terms of its importance to the organization and backup appropriately;
- Data must be stored on tapes or CDs;
- All storage media are labeled with the following information:
 - Backup date
 - Content of the backup.
- All the backups are verified to ensure the integrity of data, using the Checklist No. 1.

CONTAB

Daily Backup

- Each accounting officer is responsible, through the decision of the SAO, to create a copy (back-up) of the accounting database CONTAB-ISPA/PHARE at the end of each working day (17:00 hours), regardless of the number of recordings introduced in that certain day;
- The CD-ROM with the back-up files shall be brought to the OSO office (room no. 12, 1th floor on 44 Mircea Voda Blvd., Entrance B) by 17:15 hours;
- Immediately after receiving the back-up media containing a copy of the accounting database and software CONTAB-ISPA/PHARE, the OSO will check compliance with the procedure for completeness of the back-up (check-list completed and signed), as detailed below, and will store them in a safe place (fireproof safe) for the next two days;
- The back-up media is labelled with the following identification data:
 - date (day in which the back-up is produced),
 - back-up registration number (each back-up envelope is given an internal registration number),
 - accountant name (name of the accountant producing the back-up)
 - computer serial number (identification number of the computer whose accounting data are backed-up);
 - Considering the vulnerability of the removable media, the floppy disks used for storing the back-up data is not used more than 10-15 times and kept away from magnetic interference;

- The storing place for the daily back-up is a fireproof safe, with restricted access.

Weekly Backup

- for each accountant, a folder is created on the backup Server (\contab\back-up\\) for storing the back-up files. This folder can only be accessed by the dedicated accountant/user from his computer through the CFCU's internal computer network. The folder is shared and protected, allowing access only from the dedicated accountant's computer (based on username and password);
- In case of network failure, the back-up files will be copied using the data server's media drive. For these cases, the back-up folders are internally protected, access being allowed only upon provision of each user's password
- The server weekly back-up procedure requires the accountants to copy the back-up files on the data server inside CFCU, in the special folder created for each accountant, as follows:
 - The accountant/user creates a folder named <dd-mm-yy> in the existing dedicated folder \contab\back-up\\, to store the back-up files for a specific week;
 - The files contained on the back-up floppy disk are copied into the newly created folder: \contab\back-up\\\, either through the network, from the accountant's computer, or directly from the server's media drive, in case of network failure;

Monthly Backup

- CFCU signed an agreement with the IT General Department (ITGD) from the Ministry of Public Finance for storing back-up copies of the accounting database CONTAB-ISPA/PHARE at the end of each working week / month, regardless of the number of recordings introduced during that week / month;
- Each accounting officer is responsible, through the decision of the SAO, to create a copy (back-up) of the accounting database CONTAB-ISPA/PHARE at the end of each working week / month (Friday / last Friday of the month, 16:00 hours), after drafting of accounting statements, on a removable media (floppy disks);
- The floppy disk with the back-up files shall be brought to the OSO office (room no. 12, 1th floor on 44 Mircea Voda Blvd., Entrance B) by 16:15 hours on Friday / last Friday of each month;
- After verifying that the back-up completeness checking procedure has been fulfilled, the OSO will send the CD-ROMs to ITGD in a sealed and stamped envelope;
- The back-up media shall be labelled with the following identification data: date (day in which the back-up is produced), back-up registration number (each back-up envelope is given an internal registration number), accountant name (name of the accountant producing the back-up), computer serial number (identification number of the computer whose accounting data are backed-up);
- The OSO's nominated representative is in charge with the relationship with ITGD from the Ministry of Public Finance, being responsible with the transfer of the weekly / monthly back-up envelopes to the ITGD representative;
- An employee of ITGD is assigned as contact person and in charge with receiving and storing the envelopes containing the back-up media from the OSO's nominated representative. The envelopes are kept in a fireproof safe, with restricted access.

- Considering the vulnerability of the removable media, the floppy disks used for storing the back-up data shall not be used more than 10-15 times and kept away from magnetic interference;
- The storing place for the weekly / monthly back-up is a fireproof safe, with restricted access, within the building of ITGD;
- The period of storage is for each back-up is of three weeks / months.

Annual Backup

- CFCU signed an agreement with the IT General Department (ITGD) from the Ministry of Public Finance for storing back-up copies of the entire accounting database and software CONTAB-ISPA/PHARE at the end of each year;
- At the end of each year after drafting the annual financial statements the OSO's nominated representative will make a backup of entire accounting database and software CONTAB-ISPA/PHARE on a removable media (CD-ROMs);
- The CD-ROM with the back-up files shall be brought to the OSO office (room no. 12, 1th floor on 44 Mircea Voda Blvd., Entrance B) in the last working day of each year;
- After verifying that the back-up completeness checking procedure has been fulfilled, the OSO will send the CD-ROMs to ITGD in a sealed and stamped envelope;
- The back-up media shall be labelled with the following identification data: date (day in which the back-up is produced), back-up registration number (each back-up envelope is given an internal registration number), accountant name (name of the accountant producing the back-up), computer serial number (identification number of the computer whose accounting data are backed-up);
- The OSO's nominated representative is in charge with the relationship with ITGD from the Ministry of Public Finance, being responsible with the transfer of the yearly back-up envelopes to the ITGD representative;
- An employee of ITGD is assigned as contact person and in charge with receiving and storing the envelopes containing the back-up media from the OSO's nominated representative. The envelopes are kept in a safe place, in accordance with the Romanian regulations in force.
- Considering the vulnerability of the removable media, the CD-ROMs used for storing the back-up data shall be kept away from magnetic interference;
- The period of storage is for each yearly back-up is of ten years.

Recovery

- In case of a disaster, the Administrator can restore the application using the most recent backup file.
- The restore process is tested by the Administrator and the accounting officer is responsible for checking the completeness of the daily / weekly/monthly/annual back-ups. The following steps are to be followed in order to ensure that the back-up files are complete:
 - Before initiating the back-up procedure, the accountant makes a note on the last recording made in the accounting system, writing down the identification elements, such as: account number, the Contract number, the amount and the reference number attributed to that operation;
 - Immediately after the back-up is created, the recovery option from the accounting software is used and the back-up data stored on the CD-ROM are loaded into the system;

- The accounting officer shall verify, using the identification elements mentioned above, if the last recording made is still present in the accounting system.
- Once the recording is identified in the accounting system, the back-up is considered as complete.

Perseus

The application is installed on a computer located in the Financial Reporting Department. Being a web application, the backup is ensured by the European Commission. In case of disaster the person responsible for PERSEUS database asks Brussels for the last backup file of the database;

WebRamis

It is installed on an Olivetti computer and it is used by the Financial Department and also by the Auctions and ISPA Contracting Departments. The backup is performed weekly by copying the database manually. All the backups (daily/ weekly/ monthly/ annual) are similar with CONTAB backups.

Media

General

- The CDs are stored in a secured, lockable fireproof safe or cabinet.
- The room has air conditioning and fire extinguishers.
- The Administrator is the only one who has access to the room where the backup is stored.

Project Documentation

General

- Documentation is stored in safe lockers located in rooms with limited access. Each department has its own locker.
- The rooms where the lockers are stored have air conditioning and fire extinguishers.

User Data

Backup

- Users work and store the important data on a dedicated server (Bull 1). The folders from this server are backed-up on the server “Bull 2” daily.
- All data is classified in order of importance.
- Personnel are trained on these procedures.
- The Administrator ensures that the backup is verified.
- The Administrator is responsible for the data and information security.
- The users are responsible for their data.

Restore

- In case of disaster or hardware failure, the user asks the Administrator to restore the data using the latest backup file.

7. Training

- ITT staff regularly update their knowledge on IT security issues by participating in appropriate training programs and having access to relevant literature.
- The Administrator ensures that CFCU staff receive necessary training on IT security issues. Staff training include:
 - Updated IT procedures;
 - the nature of the threat –the reasons why IT security is important, the fact that it covers all IT systems and data and the type of attack that might compromise IT Security;
 - the importance of passwords and how to use them – stressing the need for “strong” passwords and the importance of not revealing or sharing passwords with anyone;
 - virus protection –the risks of virus attacks from email attachments, Internet downloads and software or diskettes from external sources, the basic routines to avoid them;
 - the risk of “Social Engineering” attacks – often the most secure technical solutions can be circumvented by simple trickery or deception of staff. Staff should be made aware of the dangers of this type of attack and how to guard against them;
 - secure and controllable data storage – staff shall be trained in how to properly store documents and data on the IT systems, the importance of using file servers and of filing documents in the appropriate locations on these servers.
 - after each training session the IT Team organize a testing sessions.

8. Forms

The application of the present procedure requires the following specific forms.

- ATTACHMENT 001 Annex No.1;
- ATTACHMENT 002 Annex No.2;
- ATTACHMENT 003 Request No.1;
- ATTACHMENT 004 Request No.2;
- ATTACHMENT 005 Request No.3;
- ATTACHMENT 006 Request No.4;
- ATTACHMENT 007 Checklist No.1.