HOPE'87 - IT and DISASTER RECOVERY STRATEGY

Computer Information Systems (CIS)

1. Purpose of computer information systems procedures

The purpose of computer information systems procedures is to ensure that:

- An appropriate information system is used by the organisation
- There is no unauthorised access to the organisation's computer systems
- The organisation has adequate disaster recovery plans for its computerised information
- The organisation's information is accumulated, processed and reported on accurately and in a cost-effective manner
- Personnel have adequate knowledge of the computer systems being used by the organisation

2. Computer software issues

- A decision must be made as to whether a vendor will be required to design and write a programme for the organisation or a system will be purchased off the shelf. In either case the tendering or procurement procedures, as appropriate, set out in the HOPE'87 procurement rules must be followed. In making this decision, the CIS needs of the organisation should be carefully considered
- The software used should be able to report by cost code or budget line in order to make the reports comparable to approved budgets
- The software should be configured to generate meaningful reports such as reports to donors, annual financial statements and any other report relevant for the organisation's operations, with minimum human intervention

3. Computer information systems procedures

The following procedures should be followed in order to meet the above mentioned objectives:

- Back ups of information should be carried out on a weekly basis.
- Monthly backup copies should be stored off site to ensure their safety in the event that files at the processing location are destroyed
- An anti-virus software should be loaded
- All systems should be password protected to restricted unauthorised access and to ensure the integrity of information processed and passwords should be changed on a periodic basis
- Personnel should be given the required training to properly use the systems and derive maximum benefits from it
- Access to computer information should be restricted to appropriate staff

The HOPE'87-IT system, including applications, data, hardware or communications (such as networking), is critical to the smooth operation of the organisation's daily management. Continued operation and in the event of IT-errors rapid recovery of the system has to be

HOPE'87 – General Secretariat Webpage: www.hope87.at Email: office@hope87.at
Wassergasse 29/3, 1030 Vienna, Austria
Tel: (43-1) 982 71 15 Fax: (43-1) 982 71 15 17

ensured. In the event of loss of IT infrastructure and data at HOPE'87 Headquarter as well as in the Country Offices the disaster recovery strategy comes into effect.

Disaster Recovery Strategy

1. IT- RISK ANALYSIS

Disasters can be classified in two broad categories. The first is natural disasters such as floods, earthquakes or hurricanes. While preventing a natural disaster is not possible, measures such as good planning, which includes mitigation measures, can help reduce or avoid losses. The second category is man made disasters. These include hazardous material spills, infrastructure failure or internet-terrorism.

Every HOPE'87 office, HQ as well as CO, has to conduct a thorough risk analysis of its computer system on a regular basis. All possible risks that threaten the IT-system have to be listed and their immanence has to be evaluated according to following grid:

	probability			impact		
	low	medium	high	low	medium	high
loss of electricity						
power outage						
virus attacs						
accidental data deletion						
destroyed hardware						
natural threat, eg.: earthquake, flood, fire....						
civil threat, eg.: war,....						

2. MITIGATION MEASURES

Disaster recovery planning stipulates different types of measures at different levels. These controls should be always documented and tested regularly.

2.1 Preventive measures: These controls are aimed at preventing an event from occurring

2.1.1 Each office of HOPE'87 on Country Office level as well as HQ level maintains a standby database, since this method serves as a powerful tool for both disaster prevention and reporting.

HOPE'87 – General Secretariat Webpage: www.hope87.at Email: office@hope87.at
Wassergasse 29/3, 1030 Vienna, Austria
Tel: (43-1) 982 71 15 Fax: (43-1) 982 71 15 17

2.1.2 The stand-by database has to be kept up-to-date on a regular basis. Backups have to be made at regular intervals.

2.1.3 The stand-by database has to be kept in a location that is geographically remote from the production site.

2.1.4 All staff members are regularly pointed to the risk of cyber criminality and phishing, according to the HOPE'87 guidelines on fraud and corruption.

2.2. Detective measures: These controls are aimed at detecting or discovering unwanted events

2.2.1 The stand-by database serves as protection against erroneous batch jobs or application corruptions on the production database by activating the standby before archived logs containing corrupt data are propagated.

2.2.2 Appropriate anti-virus software has to be installed and regularly updated.

2.3 Corrective measures: These controls are aimed at correcting or restoring the system after disaster or event

2.3.1 In the case of disaster, emergency operations will enter into force within the first 6 hours. After the first 48 hours most important files shall be fully restored before significant damage would be done to the organisation.

2.3.2 In the event that all media are completely destroyed at production site, the standby database can replace the destroyed or damaged database. For maximum disaster protection, data files are placed on production databases and controlled on standby databases on separate physical media in separate geographical areas.

3. THE INTENAL RISK MANAGEMENT COMMITTEE

3.1 The internal risk management committee has been established within the structure of HOPE'87.

3.2 The internal risk committee develops, supervises and reviews the organisation's IT-strategy on yearly basis.

3.3 A member of the HOPE'87 General Secretariat will serve as risk advisor.

4. VALIDITY

The IT-strategy is valid on HQ and CO level. All staff members have access to the IT-Strategy. The Country Representative has the obligation to test the accurateness of the strategy at least once a year. HQ staff members on field missions have the obligation to test the IT-recovery and backup system in the Country Office.

HOPE'87 – General Secretariat Webpage: www.hope87.at Email: office@hope87.at
Wassergasse 29/3, 1030 Vienna, Austria
Tel: (43-1) 982 71 15 Fax: (43-1) 982 71 15 17