INFORMATION SECURITY POLICY

INFORMATION BACKUPS

ISO 27002	10.5.1
Author:	Chris Stone
Owner:	Ruskwig
Organisation:	TruePersona Ltd
Document No:	SP-10.5.1
Version No:	1.0
Date:	20th December 2009

Document Control

Document Storage

Document Title Information Backups
Document Location C:\www\Ruskwig\docs\iso-27002\Information Backups - RW.doc

Version History

Version No	Version Date	Author	Summary of Changes
1.0	20/12/2009	Chris Stone	First Issue

Approvals

Name	Title	Date of Approval	Version No
Chris Stone	Director	20/12/2009	1.0

Distribution

Name	Title	Date of Issue	Version No
Everyone	Internet	29/12/2009	1.0

Contents

1. Purpose

1.1 This policy defines the strategy for backing up the organisation's information and software application systems.

1.2 The aim of the policy is to ensure that it is always possible to recover the information and application systems.

2. Scope

2.1 This policy applies to all electronic information stored upon the organisation's servers and PC's / laptops.

2.2 The policy also applies to all application systems, the application software and its configuration.

3. Risks

3.1 Information can be lost as a result of crashed disks, deletion, or corruption. Therefore, integrity and availability of important information needs to be maintained by making regular copies to other media.

4. Policy

4.1 Backup Method

4.1.1 Servers and systems will be backed up using a suitable backup method. An appropriate storage medium will be used. This may be tape, online Internet backup, mirrored servers at a remote site, or any other recognised medium.

4.1.2 Backups will be performed using dedicated backup software appropriate for the operating system being used.

4.2 Backup & Restore Procedures

4.2.1 The servers and systems will be backed up using the standard facilities available within the backup software being used.

4.2.2 Documentation with sufficient detail to allow an experienced user of the backup software to restore data will be produced.

4.3 Backup Status

4.3.1 The backup software will be configured to automatically alert an administrator as to the status of any backup performed.

4.3.2 The backup status will be reviewed on a daily basis and any faults identified will be rectified.

4.4 Verification and Restore Testing

4.4.1 Where possible the backup software will be configured to automatically verify the backup. The verification will be accomplished by comparing the contents of the backup to the data on disk.

4.4.2 The restoration of information from backup will be tested periodically.

4.5 Backup Cycles

4.5.1 Data Repository

Where possible a full backup of important systems will be taken every day. If there is insufficient available time to perform a full backup, then at a minimum a full backup will be taken weekly, with incremental backups being taken every day.

4.5.2 Rotation Scheme

Backups will utilise the grandfather, father, son (GFS) method of daily, weekly and monthly backups or a simple daily rotation method. Where a simple daily rotation method is used, at a minimum 10 backups will be kept.

4.5.3 Daily Backups

Daily backups will consist of backup taken every day as part of a simple daily rotation or as part of a GFS rotation scheme.

4.5.4 A daily backup will consist of either a full backup or an incremental / differential backup.

4.5.5 Weekly Backups

Weekly backups will consist of a 5 tape set with the tape being changed on a weekly basis.

4.5.6 A weekly backup will consist of a full backup.

4.5.7 Monthly Configuration Backup

Monthly configuration backups will consist of exporting or backing up the configuration settings of an application. The configuration will be stored on a server that is backed up daily.

4.6 Backup Storage

4.6.1 Backup media will be securely stored when not in use.

4.6.2 Online and remote disk mirroring backups will be held at a data centre at least 2km away from the data centre containing the information being backed up.

4.6.3 Removable media such as tapes will be securely stored in a fire safe when not in use.

4.6.4 For resilience several removable media will be stored offsite.

4.6.5 At a minimum two copies of the most up to date backups will be stored offsite twice a week.

4.6.6 The schedule for offsite storage will be detailed in a log.

4.7 Tape Drive Cleaning

4.7.1 Tape drives used for backups will be cleaned on a regular basis.

4.7.2 Autoloader tape drives will be cleaned weekly via a cleaning tape in the device.

4.7.3 Other tape drives will be cleaned monthly.

4.8 Application Backup

4.8.1 Use will be made of online backup techniques where they are available to minimise downtime.

4.8.2 Full offline backups will be utilised where online backups are not available.

4.9 Backup Guidelines

4.9.1 The backups of servers and applications will at a minimum comply with the following guidelines.

Server/Application	Backup Cycle	Media
Unix Apps Server	Daily	Tape/Online/Mirror
Active Directory Server	Daily	Tape/Online/Mirror
Windows File Server	Daily	Tape/Online/Mirror
Exchange Server	Daily	Tape/Online/Mirror
SQL Server	Daily	Tape/Online/Mirror
Oracle Server	Daily	Tape/Online/Mirror
Application Server data	Daily	Tape/Online/Mirror
Application Server	Daily / Weekly	Tape/Online/Mirror
DMZ Server	Weekly	Tape
Test Server	As appropriate	Tape
Firewall	Monthly Configuration	Tape
Email / Internet Gateway	Monthly Configuration	Tape
Network Switches	Monthly Configuration	Tape
VOIP Servers	Monthly Configuration	Tape

5. Enforcement

5.1 If any member of IT staff is found to have breached this policy, they may be subject to disciplinary action.

5.2 Any violation of the policy by a temporary worker, contractor or supplier may result in the termination of their contract or assignment.