INFORMATION SECURITY POLICY

REPORTING INFORMATION SECURITY INCIDENTS

ISO 27002	13.1.1
Author:	Chris Stone
Owner:	Ruskwig
Organisation:	TruePersona Ltd
Document No:	SP-13.1.1
Version No:	1.0
Date:	1st September 2009

Document Control

Document Storage

Document Title Reporting Information Security Incidents

Document Location C:\www\Ruskwig\docs\iso-27002\Reporting Information Security Incidents - RW.doc

Version History

Version No	Version Date	Author	Summary of Changes
1.0	01/09/2009	Chris Stone	First Issue

Approvals

Name	Title	Date of Approval	Version No
Chris Stone	Director	01/09/2009	1.0

Distribution

Name	Title	Date of Issue	Version No
Everyone	Internet	03/01/2010	1.0

Contents

1. Purpose

1.1 This document defines the procedure for reporting an information security incident.

2. Scope

2.1 This policy applies to all staff and employees of the organisation.

2.2 All users of the organisation's IT facilities must understand and use this policy. Users are responsible for ensuring the safety and security of the organisation's systems and the information that they use or manipulate.

2.3 All users have a role to play and a contribution to make to the safe and secure use of technology and the information that it holds.

3. Risks

3.1 Information security incidents need to be reported promptly to allow the issue to be investigated and resolved and to reduce the risk if it reoccurring.

4. Policy

4.1 An information security incident occurs when there is an event which has caused or has the potential to cause, damage to the organisation's information assets, damage to the organisation's reputation, information to be transferred to someone who is not entitled to receive it, the corruption of data.

4.2 An Information Security Incident includes:

- The loss or theft of data or information
- The transfer of sensitive or confidential information to those who are not entitled to receive that information
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system
- Changes to information or data or system hardware, firmware, or software characteristics without the organisation's knowledge, instruction, or consent
- Unwanted disruption or denial of service to a system
- The unauthorised use of a system by any person.
- Loss of service
- System malfunctions

4.3 Action on becoming aware of the incident

4.3.1 All events that could result in the actual or potential loss of data, breaches of confidentiality, unauthorised access or changes to systems should be reported immediately.

4.4 How to report

4.4.1 All suspected security events should be reported immediately to the IT Service Desk. The IT Service Desk must be contacted by email or telephone. They will log the incident and notify relevant employees and the information owner.

4.4.2 The IT Service Desk will require you to supply further information, the nature of which will depend upon the nature of the incident. However, the following information must be supplied:

- Contact name and number of person reporting the incident
- The type of data or information involved
- Whether the loss of the data puts any person or other data at risk
- Location of the incident
- Inventory numbers of any equipment affected
- Date and time the security incident occurred
- Location of data or equipment affected
- Type and circumstances of the incident.

4.4.3 Your line manager must also be informed to enable them to investigate the incident and take appropriate actions. The outcomes of these actions are to be reported to the IT Service Desk for inclusion in the incident report.

4.5 What to Report

4.5.1 All Information Security Incidents must be reported.

4.6 Examples of Information Security Incidents

4.6.1 Examples of the most common Information Security Incidents are listed below. It should be noted that this list is not exhaustive.

4.6.2 <u>Malicious Incident</u>

- Computer infected by a virus or other malware, (for example spyware or adware)
- Finding data that has been changed by an unauthorised person
- Receiving and forwarding chain letters – Including virus warnings, scam warnings and other emails which encourage the recipient to forward onto others.
- Social engineering - Unknown people asking for information which could gain them access to the organisation's data (e.g. a password or details of a third party).
- Unauthorised disclosure of sensitive or confidential information electronically, in paper form or verbally.
- Falsification of records, Inappropriate destruction of records
- Damage or interruption to the organisation's equipment or services caused deliberately e.g. computer vandalism
- Connecting third party equipment to the organisation's network
- Unauthorised Information access or use
- Giving sensitive or confidential information to someone who should not have access to it - verbally, in writing or electronically
- Printing or copying sensitive or confidential information and not storing it correctly or confidentially.

4.6.3 Access Violation

- Disclosure of logins to unauthorised people
- Writing down your password and leaving it on display or somewhere easy to find
- Accessing systems using someone else's authorisation e.g. someone else's user id and password
- Inappropriately sharing security devices such as access tokens
- Other compromise of user identity e.g. access to network or specific system by unauthorised person
- Allowing unauthorised physical access to secure premises e.g. server room, scanning facility.

4.6.4 Environmental

- Loss of integrity of the data within systems and transferred between systems
- Damage caused by natural disasters e.g. fire, burst pipes, lighting etc
- Deterioration of paper records
- Deterioration of backup tapes
- Introduction of unauthorised or untested software
- Information leakage due to software errors.

4.6.5 Inappropriate use

- Accessing inappropriate material on the internet
- Sending inappropriate emails
- Use of unapproved or unlicensed software on the organisation's equipment
- Misuse of facilities, e.g. phoning premium line numbers.

4.6.6 Theft / loss Incident

- Theft / loss of data – written or electronically held
- Theft / loss of any of the organisation's equipment including computers, monitors, mobile phones, Blackberries, Memory sticks, CDs.

4.6.7 Accidental Incident

- Sending an email containing sensitive or confidential information to 'all staff' by mistake
- Receiving unsolicited mail of an offensive nature, e.g. containing pornographic, obscene, racist, sexist, grossly offensive or violent material
- Receiving unsolicited mail which requires you to enter personal data.

4.6.8 Miskeying

- Receiving unauthorised information
- Sending sensitive or confidential information to wrong recipient.

4.6.9 Operational

- Loss of service
- System malfunction
- Uncontrolled system changes

4.7 Recording the Incident

4.7.1 The IT Service Desk will log the incident on the Incident Report form attached.

4.8 Notification

4.8.1 The IT Service Desk will notify the Information Owner and escalate the incident to the appropriate responsible officer as defined in the risk impact matrix.

4.8.2 Serious incidents should be reported to the relevant Computer Emergency Response Team (CERT).

5. Enforcement

5.1 If any user is found to have breached this security 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.

6 Definitions

6.1 Risk Impact and Responsible Manager

6.1.1 Decide upon the potential or actual impact of the information security incident using the impact matrix below and notify the appropriate responsible manager.

Type of Impact	Reputational Damage	Financial Loss / Commercial Confidentiality Loss	Disruption to Activities	Personal Privacy Infringement	Responsible Manager
Negligable	Contained internally within the organisation	Negligible	No effect on service provision	None	Head of IT
Marginal	Adverse local media	Minor	Minor disruption to service activities that can be recovered. Services slightly reduced.	Personal details revealed or compromised within department	Head of IT
Critical	Adverse national publicity	Medium	Disruption to service that can be recovered with an intermediate level of difficulty. Objectives of service not met.	Personal details revealed or compromised internally within authority. Harm mental or physical to one members of staff or public	Director
Catastrophic	Adverse international publicity	Major	Major disruption to service which is very difficult to recover from. Statutory duties not delivered.	Severe embarrassment to individual(s)	CEO

INFORMATION SECURITY INCIDENT REPORTING FORM

Incident Type			
Name of Person Reporting Incident		**Tel No**	
		Email	
Location		**Date of Incident**	
		Time of Incident	
Information Affected			
Equipment Affected			
Number of People affected		**Department Affected**	
Circumstances of the Incident			
Learning			
Further Actions			