INFORMATION SECURITY POLICY

SECURE EXTRANET ACCEPTABLE USAGE

ISO 27002	7.1.3
Author:	Chris Stone
Owner:	Ruskwig
Organisation:	TruePersona Ltd
Document No:	SP-7.1.3
Version No:	1.0
Date:	2nd September 2009

Document Control

Document Storage

Document Title Secure Extranet Acceptable Usage
Document Location C:\www\Ruskwig\docs\iso-27002\Secure Extranet AUP - RW.doc

Version History

Version No	Version Date	Author	Summary of Changes
1.0	02/09/2009	Chris Stone	First Issue

Approvals

Name	Title	Date of Approval	Version No
Chris Stone	Director	02/09/2009	1.0

Distribution

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

Contents

1. Purpose

1.1 A secure extranet is a secure private Wide-Area Network (WAN) which enables secure interactions between connected organisations.

1.2 Staff may be required to have access to the facilities operated on the secure extranet in order for them to carry out their business. This may include staff having access to a secure email facility. All staff requiring access to the secure extranet in any way will be required to read and understand this Acceptable Usage Policy (AUP).

2. Scope

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

2.2 All users of the secure extranet must understand and abide by this policy. Users are responsible for ensuring the safety and security of the secure extranet 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 The secure extranet contains sensitive information which may be put at risk if users do not follow this policy.

4. Policy

4.1 Each secure extranet user must read, understand and abide by this policy.

4.2 When using the secure extranet facilities users should comply with the following guidelines.

4.3 I acknowledge that my use of the secure extranet may be monitored and/or recorded for lawful purposes.

4.4 I agree to be responsible for any use by me of the secure extranet using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address.

4.5 I will not use a colleague's credentials to access the secure extranet and will equally ensure that my credentials are not shared and are protected against misuse.

4.6 I will protect such credentials at least to the same level of secrecy as the information they may be used to access and I will not write down or share my password.

4.7 I will not attempt to access any computer system that I have not been given explicit permission to access.

4.8 I will not attempt to access the secure extranet other than from IT equipment and systems and locations which have been explicitly authorised to use for this purpose.

4.9 I will not transmit information via the secure extranet that I know, suspect or have been advised is of a higher level of sensitivity than the secure extranet is designed to carry.

4.10 I will not transmit information via the secure extranet that I know or suspect to be unacceptable within the context and purpose for which it is being communicated.

4.11 I will not make false claims or denials relating to my use of the secure extranet.

4.12 I will protect any sensitive or confidential material sent, received, stored or processed by me via the secure extranet to the same level as I would paper copies of similar material.

4.13 I will appropriately label information using the organisation's information classification scheme.

4.14 I will not send sensitive or confidential information over public networks such as the Internet; unless it is suitably protected via encryption or other means.

4.15 I will always check that the recipients of e-mail messages are correct so that potentially sensitive or confidential information is not accidentally released into the public domain.

4.16 I will not auto-forward email from my email account to email accounts outside the organisation.

4.17 I will not forward or disclose any sensitive or confidential material received via the secure extranet unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel.

4.18 I will seek to prevent inadvertent disclosure of sensitive or confidential information by avoiding being overlooked when working, by taking care when printing information received via the secure extranet and by carefully checking the distribution list for any material to be transmitted.

4.19 I will securely store or destroy any printed material.

4.20 I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the secure extranet (this might be by logging-off from the computer, activating the password-protected screensaver, etc., so as to require a user logon for activation).

4.21 Where the IT Department has implemented other measures to protect unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked requiring a user logon for reactivation), then I will not attempt to disable such protection.

4.22 I will make myself familiar with the organisation's security policies, procedures and any special instructions that relate to the secure extranet.

4.23 I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security.

4.24 I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended.

4.25 I will not remove equipment or information from the organisation's offices without permission.

4.26 I will take precautions to protect all computer media and portable computers when taking them outside of the organisation's offices.

4.27 I will not deliberately introduce viruses, Trojan horses or other malware into the organisation's computer systems.

4.28 I will not disable anti-virus protection installed on my computer.

4.29 I will comply with legal, statutory or contractual obligations which the organisation informs me are relevant.

4.30 I will my account in accordance with the organisation's acceptable usage and security policies.

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.