ASCENT

BASE SECURITY POLICY

CONFIDENTIAL

Document type

Operational Policy

Content Outline

This document denotes the operational security aspects that Ascent adopts to safeguard confidentiality and enhance security

Last updated
31 March 2020

ISO File Format
AG011-001

Base Security

1 Information Security Policy

The Service Provider shall possess an Information Security Policy which:

i. Is endorsed by senior management

ii. Is communicated to all the organisation's employees and relevant external parties

iii. Is reviewed at planned intervals or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness

iv. Affirms management's commitment and sets out the organisation's approach to managing information security

v. Highlights the security policies, principles, standards, and compliance requirements of the organisation

vi. Highlights responsibilities of the organisation's senior management and employees vis-a-vis information security

vii. Highlights the organisation's approach towards protecting the confidentiality, integrity and availability of information it manages/operates/comes into contact with.

2 Personnel Security Screening

The Service Provider shall ensure that all employees or personnel engaged in the provision of the Services are adequately screened.

3 Information Security Awareness and Training

The Service Provider shall provide training on a continuous basis to its personnel involved in the provision of the Services in relation to the security requirements listed in this Schedule, including training on security awareness.

4 Physical and Environmental Security

The Service Provider shall:

(a). Ensure that physical controls are in place to prevent unauthorised access to Service Provider's premises.

(b). Ensure that Client Personal Data are stored in a secure manner and physically protected from unauthorised access and damage.

5 Secure Disposal or Re-use of Equipment

The Service Provider shall ensure the secure disposal or re-use of all hardware used that contains Client Personal Data, if applicable.

6 Secure Disposal of Media

The Service Provider shall implement mechanisms for Client Personal Data to be removed or securely overwritten to reduce the possibility of recovery. The mechanisms used to delete Client Personal Data shall be commensurate to the sensitivity of the data concerned.

7 Separation of Development and Operational Facilities

If applicable, the Service Provider shall maintain development, operational and test environments separate to reduce risks of unauthorised access or changes.

8 Clock Synchronisation

The Service Provider shall ensure that clocks are synchronized with an accurate time-source.

9 Clear-desk and clear screen

The Service Provider shall ensure that that papers and storage media containing Client Personal Data is stored in a secure manner (e.g. in locked cabinets) when not in use to reduce risks of unauthorised access, loss or damage to the Client Personal Data. During the time that a machine/device is connected to Client's network or access Client Personal Data, such machine/device should not be left unlocked.

10 Business Continuity Management, including Disaster Recovery

The Service Provider shall:

(a). Develop and maintain, throughout the term of the Principal Agreement, appropriate business continuity and/or disaster recovery plans;

(b). Test the business continuity and/or disaster recovery plans on a regular basis and in any event not less than once in every calendar year.

11 Passwords

The Service Provider shall ensure that all devices utilised by its personnel to access Client Personal Data are password protected to prevent unauthorised access.

12 Access control to program source code

The Service Provider shall ensure that access to its proprietary Solution's source code is restricted.

13 Access Control

The Service Provider shall ensure that its personnel having access to Client Personal Data are granted minimum rights and privileges required to execute their duties, as per least privilege principle.

14 Protection of System test data

The Service Provider shall, as far as reasonable practicable, use test data for testing purposes. Where test data cannot be used, the Service Provider shall with the prior approval of the Client use live data that is sanitised or, only where strictly necessary, use live data on a test environment that shall have the same level of security controls as in the operational environment. The Service Provider shall delete any live data once testing is completed and shall inform the Client in writing of such deletion for audit trail purposes.

15 Server and Database Hardening

The Service Provider shall:

(a). Ensure traceability by enabling operating system security audit logs on servers.

(b). Implement database hardening mechanisms to safeguard sensitive fields/records within the database.

16 Remote Access Control

In the event that the Service Provider requires remote access to Client's Network, the following conditions must be observed:

(a). A request must be submitted by the Service Provider to the Client identifying the person(s) who will be accessing the Client's Network, the purpose of the request/access and the period for which access is required. The request must be formally authorised by the Client's department manager or the CTO. The request and approval may be provided by means of electronic mail.

(b). In order to ensure individual accountability of the activity carried out on Client's Network by Service Provider personnel, Service Provider's personnel are to be given unique userid and passwords.

(c). The 'least privilege principle' approach shall be adopted, unless specific circumstances mandate otherwise.

(d). Network connectivity to Client Network shall be provided through access methods meeting appropriate security protocols, particularly that the authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks.

(e). It is being agreed, notwithstanding the aforementioned the Parties agree that the following tools may be used:

i. TeamViewer
ii. GoToMeeting
iii. GoToMyPc
iv. Skype
v. Skype for Business
vi. VMWare Horizon
vii. OpenVPN
viii. Shrew soft VPN Access Manager
ix. VNC
x. Windows Remote Desktop Connection
xi. Secure FTP using Secure Shell protocol (SFTP SSH)

(f). Without prejudice to the above, all Service Provider hosts connected to the Client's Network must:

i. Use the most up-to date anti-virus and anti-malware available
ii. Be protected by a corporate firewall and
iii. Be up to date with operating system patches