Insuletics Limited

IT Information Security Policy

IT Policy	**1**
Appendix	***2***
Issue	**2**
Approved by:	**Ian Coates**

1. Purpose and Objectives

The Information Security Policy is to enable all users to meet their responsibilities for the security of Insuletics information held in electronic formats.

This policy must be read in conjunction with the Procedures for the Information Communication Technology Security and other associated Procedures and Guidelines.

2. Definitions, Terms, Acronyms

ICT Asset - All applications and technologies that are owned procured and/or managed by Insuletics. These include desktop and productivity tools, application environments, hardware devices and systems software, network and computer accommodation, and management and control tools.

Information - Any collection of data that is processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.

Information Asset - An identifiable collection of data stored on ICT Assets and recognised as having value for the purpose of enabling Insuletics to perform its business functions, thereby satisfying a recognised requirement.

Information Security - Concerned with the protection of information from unauthorised use or accidental modification, loss or release.

Information Systems - The organised collections of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information.

Secure Area - Provides the highest integrity of access to, and audit of, Security Classified Information Assets to ensure restricted distribution and to assist in subsequent investigation if there is unauthorised disclosure or loss of information assets. The essential physical security features of a Secure Area include:

- appropriately secured points of entry and other openings
- an effective means of providing access control during both operational and non-operational hours
- all visitors escorted at all times
- during non-operational hours a monitored security alarm system, providing coverage for all areas where Security Classified information assets are stored
- an approved means of limiting entry to authorised persons.

3. Policy Scope/Coverage

This policy applies to system owners and staff responsible for implementation and maintenance of information assets and ICT assets.

4. Policy Statement

Insuletics policy on information security in respect of policy, planning, asset management, human resources management, physical and environmental management, communications and operations management, access management, system acquisition, development and maintenance, incident management, business continuity management, and compliance management.

The policy recognises that effective IT security involves the cooperation of all staff and depends on responsible use of Insuletics IT systems by its users.

Security should be pragmatic and not unduly compromise the principle of providing staff and other authorised users with access to accurate, relevant and timely information.

Information Security Policy is directed at the preservation of the following principles:

- Confidentiality: ensuring that information is accessible only to those authorised to have access.
- Integrity: safeguarding the accuracy and completeness of information and processing method.
- Availability: ensuring that authorised users have access to information and associated systems when required.

Responsible use: ensuring that controls are in place so that users of Insuletics systems are not able to affect adversely other users or other systems.

Compliant Use: meeting legal and contractual obligations.

5. Policy, Planning and Governance

5.1 Information security policy

This policy will be communicated on an ongoing basis and be accessible to all

5.2 Information security plan

Insuletics Information Security Plan must align with its Mission Statement, Strategic Plan and risk assessment findings. The Guideline provides further information.

A threat and risk assessment must be conducted for all ICT assets that create, store, process or transmit Security Classified Information.

5.3 Internal ICT governance

Roles and responsibilities to implement, maintain and control operational information security are detailed in The Procedure.

5.4 External party ICT governance

Third party service level agreements, operational level agreements, hosting agreements or similar contracts must clearly articulate the level of security required.

6. Asset Management

6.1 ICT asset protection responsibility

- All ICT assets that create, store, process or transmit Security Classified Information must be assigned appropriate controls.
- A brief overview of the controls applicable to the security classifications of the majority of Insuletics Information is contained in The Guideline.
- All ICT assets that provide underpinning (core) and ancillary services must be protected from internal and external threats (e.g. mail gateways, domain name resolution, time, reverse proxies, remote access and web servers).

6.2 Information security classification

- Timeframes for implementation are outlined in The Guideline.
- Classification schemes do not limit the applicability of relevant legislation.

7. Human Resources Management

7.1 During employment

All employees must be made aware of Insuletics ICT information security policy, their security responsibilities, and associated security processes.

7.2 Upon Termination of Employment

Upon termination of employment, the member of staff will have his/her access to all computer terminals, secure areas revoked immediately.

8. Physical and Environmental Management

8.1 Building controls and secure areas

Building and entry controls for areas used in the processing and storage of ICT Information must be established and maintained as outlined in The Guideline.

8.2 Equipment security

All ICT assets that store or process information must be located in Secure Areas with control mechanisms in place to restrict access to authorised personnel only.

- Policies and processes must be implemented to monitor and protect the use and/or maintenance of Information Assets.
- Policies and processes must be implemented to securely dispose and/or reuse ICT assets as referenced in The Procedure.

9. Communications and Operations Management

9.1 Operational procedures and responsibilities

All information assets and ICT assets (including networks and methods for exchanging information) must be managed securely and consistently (in accordance with the level of security required).

Operational change control procedures must be implemented to ensure that changes to information processing facilities or systems are appropriately approved and managed.

9.2 Third party ICT service delivery

Third party service delivery agreements must comply with Insuletics Information Security Policy.

9.3 Capacity planning and system acceptance

System acceptance must include confirmation of the application of appropriate security controls and of the capacity requirements of the system.

System capacity must be regularly monitored to ensure risks of system overload or failure which could lead to a security breach are avoided.

9.4 Application integrity

Adequate controls must be defined and implemented for the prevention, detection; removal and reporting of attacks by malicious code on all ICT assets.

Vulnerability/integrity scans of core software must be conducted regularly to ensure detection of unauthorised changes.

Anti-malicious-code software must be regularly updated with new definition files and scanning engines.

Employees must be educated about malicious code, the risks posed, virus symptoms and warning signs including what processes should be followed in the case of a suspected virus.

9.5 Backup procedures

Comprehensive information and system backup procedures must be implemented.

9.6 Network security

A procedure on scanning must be implemented to ensure that traffic entering and leaving the Insuletics network is appropriately scanned for malicious or unauthorised content.

9.7 Information exchange

Methods for exchanging information through online services, and/or with third parties must be compliant with legislative requirements.

9.8 Information processing monitoring

ICT assets must be synchronised to a trusted time source.
Operator and audit/fault logs must be implemented on Information Systems.

10. Access Management

10.1 Access control policy

Control mechanisms based on business requirements and assessed/accepted risks for controlling access to all corporate information assets and ICT assets must be established.

Access control rules must be consistent with Insuletics business requirements, information classification, and legal/legislative obligations.

10.2 Authentication

Authentication requirements including on-line transactions and services must be appropriate for the security classification of the information.

10.3 User access

Access to information systems requires specific authorisation and each user must be assigned an individually unique personal identification code and secure means of authentication.

10.4 User responsibilities

Users are responsible for complying with The Procedure and the Use of ICT Policy and related documents.

10.5 Network access

- Authorisation must be obtained and documented for access (including new connections) to Insuletics networks.
- All wireless communications must have appropriate configured product security features and afford at least the equivalent level of security of wired communications.
- Remote access to Insuletics core business systems requires authentication and use of encrypted tunneling technology.

10.6 Operating system access

ICT assets utilising Insuletics sign-in have standard user registration, authentication management, access rights and privileges implemented.

10.7 Application and information access

Restricted access and authorised use only warnings must be displayed upon access to all systems which have this capability.

Access to all confidential/sensitive systems requires authorised approval.

10.8 Mobile computing access

Processes must be established for mobile facilities.

11. System Acquisition, Development and Maintenance

11.1 System security requirements

Security controls must be commensurate with the Security Classifications of the information contained within, or passing across information systems, network infrastructures and applications.

Security requirements must be addressed in the specifications, analysis and/or design phases and internal and/or external audit must be consulted when implementing new or significant changes to financial or critical business information systems.

Security controls must be established during all stages of system development, as well as when new systems are implemented and maintained in the operational environment.

Appropriate change control, acceptance and system testing, planning and migration control measures must be carried out when upgrading or installing software in the operational environment.

11.2 System files

Access to system files must be controlled to ensure integrity of the business systems, applications and data.

11.4 Secure development and support processes

Processes (including data validity checks, audit trails and activity logging) must be established in business critical applications to ensure development and support processes do not compromise the security of applications, systems or infrastructure.

11.5 Technical vulnerability management

- Processes to manage software vulnerability risks must be developed and implemented.
- A patch management program for operating systems, firmware and applications of all ICT assets must be implemented to maintain vendor support, increase stability and reduce the likelihood of threats being exploited.

12. ICT Incident Management

12.1 Event/weakness reporting

- An information security incident register must be maintained and all incidents recorded
- All information security incidents must be reported and escalated (where applicable) through appropriate management channels and/or authorities.
- Where a deliberate violation or breach of information security policy or subordinate processes has occurred, this must be investigated and appropriate action taken.

- Responsibilities and procedures for the timely reporting of security events and incidents including breaches, threats and security weaknesses, must be communicated to all employees including contractors and third parties.

12.2 Incident procedures

Information security incident management procedures must be established to ensure appropriate responses in the event of information security incidents, breaches or system failures.

13. Business Continuity Management

13.1 ICT disaster recovery

Methods must be developed to reduce known risks to information and ICT assets.

14. Compliance Management

14.1 Legal requirements

- All legislative obligations relating to ICT information security must be complied with and managed appropriately.
- All information security policies, processes and requirements including contracts with ICT third parties, must be reviewed for legislative compliance on a regular basis.

14.2 Policy requirements

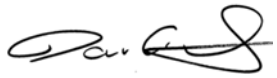
All reporting obligations relating to ICT information security must be complied with and managed appropriately.

14.3 Audit requirements

All reasonable steps must be taken to monitor, review and audit Insuletics ICT information security compliance, including the engagement of internal and/or external auditors and specialist organisations where required.

Date: 3rd November 2014

Signed:



Ian Coates
Managing Director