OCORIAN

Ocorian Corporate Services (Mauritius) Limited

INFORMATION SECURITY POLICY

25 September 2018

INTRODUCTION

As part of Ocorian Corporate Services (Mauritius) Limited Information Security Management System, Ocorian has drafted this Policy document, which describes its policies in terms of information security. The policies described below are derived from the ISO/IEC 27001:2013 standard.

OBJECTIVES

The objectives of Ocorian Corporate Services (Mauritius) Limited Information Security Management System ('ISMS') are to:

- Ensure that Ocorian information systems safeguard and protect client data;
- Provide a secure and structured information management and archiving system;
- Ensure compliance with information security laws and regualtions;
- Obtain and maintain the ISO 27001 certification at Ocorian; and
- Build an information security culture within the organisation.

1. INFORMATION SECURITY POLICIES

1.1 Policies for Information Security

Ocorian shall define a set of policies for information security, which shall be approved by management, published and communicated to employees and relevant external parties.

1.2 Review of the Policies for Information Security

The policies for information security shall be reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability, adequacy and effectiveness.

2. INTERNAL ORGANISATION OF INFORMATION

2.1 Information Security Roles and Responsibilities

Ocorian shall define and allocate all information security responsibilities.

2.2 Segregation of Duties

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.

2.3 Contact with Authorities

Ocorian shall maintain appropriate contacts with relevant authorities.

2.4 Contact with Special Interest Groups

Ocorian shall maintain appropriate contacts with special interest groups or other specialist security forums and professional associations.

2.5 Information security in project management

Ocorian shall ensure that information security is addressed in project management, regardless of the type of project.

3. MOBILE DEVICES AND TELEWORKING

3.1 Mobile Device Policy

Ocorian shall adopt a policy and supporting security measures to manage the risks relating to mobile devices.

3.2 Teleworking

Ocorian shall implement a policy and supporting security measures to protect information accessed, processed or stored at teleworking sites.

4. HUMAN RESOURCE SECURITY

4.1 Screening

Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and perceived risks.

4.2 Terms and Conditions of Employment

The contractual agreements with employees and contractors should state their and Ocorian responsibilities for information security.

4.3 Management Responsibilities

Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of Ocorian.

4.4 Information security awareness, education and training

All employees of Ocorian and contractors should receive appropriate awareness education and training and regular updates in Ocorian policies and procedures, as relevant to their job function.

4.4 Disciplinary Process

There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.

4.5 Termination or change of employment responsibilities

Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to all employees and contractors of Ocorian, and shall be enforced.

5. ASSET MANAGEMENT

5.1 Inventory of Assets

Assets associated with information and information processing facilities at Ocorian shall be identified and an inventory of these assets should be drawn up and maintained.

5.2 Ownership of Assets

Assets maintained in the inventory shall be owned by the relevant function or person at Ocorian.

5.3 Acceptable Use of Assets

Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.

5.4 Return of Assets

All employees of Ocorian and external party users shall return all Ocorian assets in their possession upon termination of their employment, contract or agreement.

5.5 Classification of Information

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

5.6 Labelling of Information

An appropriate set of procedures for information labellling should be developed and implemented in accordance with the information classification scheme adopted by Ocorian.

5.7 Handling of assets

Procedures for handling assets should be developed and implemented in accordance with the information classification scheme adopted by Ocorian.

5.8 Management of removable media

Procedures should be implemented for the management of removable media in accordance with the classification scheme adopted by Ocorian.

5.9 Disposal of Media

Media should be disposed of securely when no longer required, using the formal procedures established at Ocorian.

5.10 Physical Media Transfer

Media containing information should be protected against unauthorised access, misuse or corruption during transportation in and out of Ocorian.

6. ACCESS CONTROL

6.1 Access control policy

An access control policy shall be established, documented and reviewed based on business and information security requirements of Ocorian.

6.2 Access to networks and network services

Users at Ocorian should only be provided with access to the network and network services that they have been specifically authorised to use.

6.3 User registration and de-registration

A formal user registration and de-registration shall be implemented at Ocorian to enable assignment of access rights.

6.4 User access provisioning

A formal user access provisioning process shall be implemented at Ocorian to assign and revoke access rights for all user types to all systems and services.

6.5 Management of privileged access rights

The allocation and use of privileged rights shall be restricted and controlled.

6.6 Management of secret authentication information of users

The allocation of secret authentication information shall be controlled through a formal management process.

6.7 Review of access rights

All asset owners at Ocorian shall review users' access rights at regular intervals.

6.8 Removal or adjustment of access rights

The access rights of all employees at Ocorian and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon charge.

6.9 Use of secret authentication information

Users at Ocorian shall be required to follow the defined practices in the use of secret authentication information.

6.10 Information access restriction

Access to information and application system functions shall be restricted in accordance with the access control policy of Ocorian.

6.11 Secure log-on procedures

Where required by the access control policy, access to systems shall be controlled a secure log-on procedure.

6.12 Password management system

Password management systems should be interactive and should ensure quality passwords

6.13 Use of privileged utility programs

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

6.14 Access control to program source code

Access to program source code shall be restricted.

7. CRYPTOGRAPHY

7.1 Cryptographic controls

Ocorian shall develop and implement a policy on the use of cryptographic controls for protection of information.

7.2 Key management

Ocorian shall develop and implement a policy on the use, protection and lifetime of cryptographic keys through their whole lifecycle.

8. PHYSICAL AND ENVIRONMENTAL SECURITY

8.1 Physical Security Perimeter

Security perimeters shall de defined and used to protect information processing facilities and areas that contain either sensitive or critical information.

8.2 Physical entry controls

Secured areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

8.3 Securing offices, rooms and facilities

Physical security for offices, rooms and facilities shall be designed and applied.

8.4 Protecting against external and environmental threats

Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.

8.5 Working in secure areas

Ocorian shall design and apply procedures for working in secure areas.

8.6 Delivery and loading areas

Access points such as delivery and loading areas and other points where unauthorised persons could enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

8.7 Equipment siting and protection

Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

8.8 Supporting utilities

Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

8.9 Cabling security

Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.

8.10 Equipment maintenance

Equipment shall be correctly maintained to ensure its continued availability and integrity.

8.11 Removal of assets

Equipment, information or software shall not be taken off-site without prior authorisation.

8.12 Security of equipment and assets off-premises

Security shall be applied to off-site assets taking into account the different risks of working outside the Ocorian's premises.

8.13 Secure disposal or re-use of equipment

All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

8.14 Unattended user equipment

Users at Ocorian shall ensure that unattended equipment has appropriate protection.

8.15 Clear desk and clear screen policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.

9. OPERATIONS SECURITY

9.1 Documented operating procedures

Operating procedures shall be documented and made available to all users who need them.

9.2 Change management

Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled.

9.3 Capacity management

The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

9.4 Separation of development, testing and operational environments

Development, testing, and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment.

9.5 Protection from malware

Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

9.6 Information backup

Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.

9.7 Event logging

Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

9.8 Protection of log information

Logging facilities and log information shall be protected against tampering and unauthorised access.

9.9 Administrator and operator logs

System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.

9.10 Clock synchronization

The clocks of all relevant information processing systems within Ocorian shall be synchronised to a single reference time source.

9.11 Installation of software on operational systems

Procedures shall be implemented to control the installation of software on operational systems.

9.12 Management of technical vulnerabilities

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, Ocorian's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

9.13 Restrictions on software installation

Rules governing the installation of software by users shall be established and implemented.

9.14 Information systems audit controls

Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.

10. COMMUNICATIONS SECURITY

10.1 Network controls

Networks shall be managed and controlled to protect information in systems and applications.

10.2 Security of network services

Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.

10.3 Segregation in networks

Groups of information services, users and information systems shall be segregated on networks.

10.4 Information transfer policies and procedures

Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

10.5 Agreements on information transfer

Agreements shall address the secure transfer of business information between the organization and external parties.

10.6 Electronic Messaging

Information involved in electronic messaging shall be appropriately protected.

10.7 Confidentiality and non-disclosure agreements

Requirements for confidentiality or non-disclosure agreements reflecting the Ocorian's needs for the protection of information shall be identified, regularly reviewed and documented.

11. SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

11.1 Information security requirements analysis and specification

The information security related requirements shall be included in the requirements for new

information systems or enhancements to existing information systems.

11.2 Securing application services on public networks

Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

11.3 Protecting application services transactions

Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

11.4 Secure development policy

Rules for the development of software and systems shall be established and applied to developments within the organization.

11.5 System change and control procedures

Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.

11.6 Technical review of applications after operating platform changes

When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

11.7 Restrictions on changes to software packages

Modifications to software packages shall be discouraged, limited to necessary changes and all changes should be strictly controlled.

11.8 Secure system engineering principles

Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.

11.9 Secure development environment

Ocorian shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.

11.10 Outsourced development

Ocorian shall supervise and monitor the activity of outsourced system development.

11.11 System security testing

Testing of security functionality shall be carried out during development.

11.12 System acceptance testing

Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.

11.13 Protection of test data

Test data shall be selected carefully, protected and controlled.

12. SUPPLIER RELATIONSHIPS

12.1 Information security policy for supplier relationships

Information security requirements for mitigating the risks associated with supplier's access to the Ocorian assets shall be agreed with the supplier and documented.

12.2 Addressing security within supplier agreements

All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for Ocorian information.

12.3 Information and communication technology supply chain

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.

12.4 Monitoring and review of supplier services

Ocorian shall regularly monitor, review and audit supplier service delivery.

12.5 Managing changes to supplier services

Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

13. INFORMATION SECURITY INCIDENT MANAGEMENT

13.1 Responsibilities and procedures

Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.

13.2 Reporting information security events

Information security events shall be reported through appropriate management channels as quickly as possible.

13.3 Reporting information security weaknesses

Employees and contractors using the Ocorian information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.

13.4 Assessment of and decision on information security events

Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.

13.5 Response to information security events

Information security incidents shall be responded to in accordance with the documented procedures.

13.6 Learning from information security incidents

Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.

13.7 Collection of evidence

Ocorian shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.

14. INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

14.1 Planning information security continuity

Ocorian shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.

14.2 Implementing information security continuity

Ocorian should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

14.3 Verify, review and evaluate information security continuity

Ocorian shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.

14.4 Availability of information processing facilities

Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

15. COMPLIANCE

15.1 Identification of applicable legislation and contractual requirements

All relevant legislative statutory, regulatory, contractual requirements and the Ocorian's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and for Ocorian.

15.2 Intellectual property rights

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

15.3 Protection of records

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorised release, in accordance with legal, regulatory, contractual and business requirements.

15.4 Privacy and protection of personally identifiable information

Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.

15.5 Regulation of cryptographic controls

Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.

15.6 Independent review of information security

Ocorian approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

15.7 Compliance with security policies and standards

Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

15.8 Technical compliance review

Information systems shall be regularly reviewed for compliance with the Ocorian information security policies and standards.