Information Security Policy

Purpose

This policy was developed to communicate to all relevant stakeholders (employees, contractors, consultants, temporaries, and applicable suppliers/vendors) the measures Deluxe requires for securing information and information processing. It is a key component of Deluxe's overall Information Security management framework and is supported by more detailed information security documentation including security standards, specifications, and procedures.

This policy is designed to meet or exceed the guidance found in existing laws and regulations. If any content of this policy conflicts with applicable state/province or federal/national law, the applicable law will supersede. If any content in this policy is stricter than applicable law and such a law does not preclude application of stricter requirements, then the policy will apply.

Background

The objective of this policy is to establish and maintain the confidentiality, integrity and availability of Deluxe resources in accordance with industry standard best practices by:

- Ensuring that all relevant stakeholders are aware of, and fully comply with, requirements as described in this document
- Introducing a consistent approach to security, ensuring that all members of the staff fully understand their responsibilities
- Creating and maintaining a level of awareness of information security as an integral part of day-to-day business
- Protecting information assets under the control of the organization

The centrally posted electronic copy of the Deluxe Information Security Policy on Inside Deluxe is the only official version of the document. Printed copies are not considered official.

IT Senior Leadership Team (IT SLT) or Executive Leadership Team (ELT) may require an independent review of the information security program to ensure the continuing suitability, adequacy and effectiveness of Deluxe's approach.

Reviews will be carried out by individuals independent of the area under review, such as Assurance & Risk Advisory Services, a manager, or a third-party organization specializing in such reviews. Individuals carrying out these reviews are required to have the appropriate skills and experience.

Scope	This Policy applies to all Deluxe employees, contractors, consultants, temporaries, and applicable suppliers/vendors.
Definitions	**Asset:** Anything of value or usefulness such as information, major applications, general support systems, physical plants or facilities, personnel, equipment, or a logically related group of systems. **Information Security:** Organizational function that protects information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction to provide integrity, confidentiality and availability. **Owner:** A person or unique role within Deluxe, that has primary accountability for the viability, productivity, and resilience of an organizational asset.
Information Security Requirements	Deluxe's Information Security requirements are documented in this policy with supporting standards and specifications. These standards are available on Inside Deluxe. **5. Information Security Policies** Deluxe will manage information security policy and standards to provide management direction and support for information security in accordance with business requirements, relevant laws and regulations. **6. Organization of Information Security** Deluxe will establish a management framework for managing information security risk. Deluxe will: • Ensure that information security responsibilities are defined and allocated, including for the acceptance of residual risk • Segregate conflicting duties and areas of responsibility • Maintain appropriate contact with authorities, professional groups, and associations • Address information security requirements in project management, ensuring information security risk is identified and addressed • Maintain security measures to manage the risk of mobile devices and teleworking **7. Human Resource Security**

Deluxe will ensure that all relevant stakeholders are aware of information security threats, aware of their responsibilities, and are equipped to support this information security policy. Deluxe will:

- Ensure relevant stakeholders understand their responsibilities and are suited for the roles for which they are considered
- Implement background verification checks in accordance with relevant laws, regulations, and ethics
- Include employee, temporary, and contractor information security responsibilities in contractual obligations
- Ensure employees and contractors are aware of, and fulfill, their information security responsibilities
- Provide information security awareness, education, and training
- Protect the security of information during change, or termination, of employment

Deluxe will have a formal, communicated disciplinary process to address security violations.

8. Asset Management

Deluxe will take appropriate measures to effectively and securely manage Deluxe assets. Deluxe will:

- Establish requirements for identification of organizational assets and definitions of appropriate protection measures
- Define a classification schema to ensure information receives an appropriate level of protection in accordance with the importance of the data and level of risk
- Take reasonable measures to prevent the unauthorized disclosure, modification, removal or destruction of information

Asset Owners will be identified. Delegation of ownership responsibilities is permitted; however, accountability will be maintained at the appropriate level.

9. Access Control

Deluxe will limit and control access to information and information processing facilities. Deluxe will:

- Establish, document and review access appropriate to the role
- Provide access to the network and network services when specifically authorized
- Develop and maintain processes to ensure authorized users can access information, systems and services to do their job
- Inform and hold personnel accountable for safeguarding sensitive information, including secret authentication information
- Take reasonable measures to prevent unauthorized access to systems and applications

10. Cryptography

Deluxe will ensure the proper use of cryptographic techniques to protect the confidentiality, availability and integrity of sensitive information. Deluxe will:

- Use cryptology to properly and effectively ensure confidentiality, integrity/authenticity, non-repudiation, authentication and access control
- Develop, document, and implement processes on the use, protection and lifecycle of cryptographic keys

11. Physical and Environmental Security

Deluxe will define measures or controls to protect Deluxe facilities and equipment. Deluxe will:

- Take reasonable measures to prevent unauthorized physical access, damage and interference to Deluxe's information and information processing facilities.
- Take reasonable measures to prevent loss, damage, theft or compromise of assets or interruption to Deluxe's operations.

Deluxe employees, contractors, consultants, temporaries, and applicable suppliers/vendors will maintain a clean desk and clear screen, considering the information classification, legal/contractual requirements and the corresponding risks.

12. Operations Security

Deluxe will take reasonable measures to provide a robust, reliable and secure IT infrastructure that protects information. Deluxe will:

- Document procedures to ensure correct and secure operations or information processing facilities with the capacity to ensure required system performance
- Control change through a formal change management process
- Maintain separate environments for development, testing and production
- Implement reasonable controls to protect against malware and protect against data loss
- Log and monitor information security events, protect logs against tampering and unauthorized access, and synchronize clock mechanisms
- Implement procedures to control installation of software
- Manage technical vulnerabilities
- Plan to minimize the impact of audit activities on operational systems

13. Communications Security

Deluxe will ensure the protection of information in networks and supporting information processing facilities. Deluxe will:

- Implement network security controls to protect information networks and supporting processing facilities
- Maintain the security of information transferred within the organization and with external entities

14. System Acquisition, Development and Maintenance

Deluxe will ensure that security is part of system development and system maintenance activities. Deluxe will:

- Ensure that information security is an integral part of information systems across the entire lifecycle and includes requirements for information systems which provide services over public networks
- Ensure information security is designed and implemented within the development lifecycle of information systems
- Define and implement requirements for protection of data used for testing

15. Supplier Relations

Deluxe will take appropriate measures to protect information when engaging suppliers with access to organizational assets and information. Deluxe will:

- Take appropriate measures to protect supplier access to organizational assets and information
- Maintain an agreed upon level of information security and service delivery in line with supplier agreements and the risk posed by the supplier

16. Information Security Incident Management

Deluxe will restore normal service operations as quickly as possible and minimize adverse impact on business operations, ensuring agreed levels of service quality are met. Deluxe will:

- Establish a consistent and effective approach to the management of information security incidents, including communication of security events and weaknesses

17. Information Security Aspects of Business Continuity

Deluxe will ensure that interruptions to normal operations are minimized and that critical resources and processes are protected from the effects of major failures or disasters. Deluxe will:

- Embed information security continuity requirements into Deluxe's business continuity management
- Ensure availability of information processing facilities

18. Compliance

Deluxe will ensure that operations and systems conform to legal, regulatory and internal security requirements. Deluxe will:

- Set standards to help prevent breaches of legal, statutory, regulatory or contractual obligations related to information security.
- Ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Anti-retaliation	Deluxe prohibits any form of retaliation for reporting a suspected violation of this Policy made in good faith.
Policy compliance and exceptions	All employees, contractors, consultants, temporaries, and applicable suppliers/vendors are responsible for enforcement of, and compliance with, this Policy, including its communication to their employees. Managers must document any requests for exceptions to the policy and provide a valid business justification or constraints that prevent complete compliance. Exceptions must be approved by appropriate levels of management based on risk. Anyone who does not comply with this Policy shall be subject to disciplinary action, up to and including termination, to the extent permissible under local law. Vendors failing to meet security obligations could be subject to contract termination. If you have information about a possible violation of this Policy, contact Information Security, the Deluxe Hotline, or the vendor relationship manager.
Review schedule	This policy is reviewed annually, or as required by circumstances or operation of law.