enfinium	**Information Security Policy**	
IT-POL-001	Rev. 1.1	**Information Technology**

1. PURPOSE

The Information Security Policy defines the requirements for creating and maintaining a strong information security position through the application of information security controls, information ownership and information protection. IT applies to enfinium information assets. Implementation of this policy is intended to significantly reduce risk to the confidentiality, integrity and availability of enfinium information systems and resources that enable achievement of enfinium's strategic and operational business objectives.

2. SCOPE

It is the responsibility of each enfinium employee, consultant and contractor to read and understand this Policy as well as the associated procedures and documentation that will implement it. Management is accountable for implementing and supporting this Policy.

3. REFERENCES

Document Number	Title
HR-POL-021	Business Ethics and Conflicts of Interest Policy
LEG-POL-005	Data Retention Period Statement
IT-POL-003	Acceptable Use Policy
IT-POL-006	Password Policy

4. DEFINITIONS

Term	Definition
n/a	

5. RESPONSIBILITIES

5.1. Change Configuration Review Board

5.1.1. Members of the Board shall ensure that the necessary controls are implemented and complied with as per this policy.

5.2. IT Manager

5.2.1. Establish and revise the information technology strategy, policy and standards for change management and control with input from interest groups and subsidiaries;

5.2.2. Facilitate and co-ordinate the necessary counter measures to change management and control initiatives and evaluate such policies and standards;

5.2.3. Establish the security requirements for change management and control directives and approval of the change management and control standards and change control/ version control products;

5.2.4. Co-ordinate the overall communication and awareness strategy for change management;

5.2.5. Acts as the management champion for change management and control;

5.2.6. Provide technical input to the service requirements and co-ordinate affected changes to SLA's where applicable.

5.2.7. Establish and co-ordinate appropriate interest group forums to represent, feedback, implement and monitor change management and control initiatives;

5.2.8. Ensure that all application owners are aware of the applicable policies, standards, procedures and guidelines for change management and control;

5.2.9. Co-ordinate the implementation of new or additional security controls for change management; and

5.2.10. Approve and authorise change management and control measures on behalf of enfinium.

5.3. IT Service Provider

5.3.1. Shall comply with all change management and control statements of this policy.

5.4. Solution Owners

5.4.1. Shall comply with all information security policies, standards and procedures for change management and control; and

5.4.2. Report all deviations.

6. POLICY STATEMENT

6.1. DATA CLASSIFICATION

enfinium classifies information within the scope of our Data Retention Period Statement by the level of sensitivity. That way we can appropriately allocate resources for the protection of each type of asset or media through a range of controls, policies, processes, procedures, organizational structures, training, software, hardware and network functionality and design.

6.2. POLICY

enfinium shall establish and maintain comprehensive protection and clear accountability for all enfinium information assets and resources. This includes information assets that are proprietary to enfinium, private to enfinium customers and partners, and all other private and proprietary information and assets and resources that, if subject to inadvertent or unauthorized access or disclosure, would likely cause financial, legal, or reputational damage to enfinium or enfinium customers and partners.

6.3. APPLICABILITY

This Policy and associated standards, procedures and guidelines apply to all enfinium employees, contractors, sub-contractors, and their respective facilities supporting enfinium business operations, wherever enfinium data is stored or processed, including any third-party contracted by enfinium to handle, process, transmit, store, or dispose of enfinium data.

6.4. LEADERSHIP AND COMMITMENT

enfinium's Senior Leadership Team is committed to promoting information security and privacy objectives globally. This commitment is demonstrated through their support of the Information Security Management System (ISMS) operations; encouraging a culture of security vigilance; their provisioning of the appropriate resources required to develop and maintain the ISMS, as well as their support of legal, contractual and customer experience endeavours. enfinium's Senior Leadership Team is involved in the establishment and ongoing maintenance of Information Security and data protection at enfinium. The committee understands that enfinium must:

"secure our technologies and facilities in order that enfinium provides an easy to use and safe experience for enfinium's customers, partners and staff that meets and exceeds the level of acceptable risk appropriate to a waste to energy business."

6.5. NON-COMPLIANCE

In the absence of an approved exception, failure to comply may be considered a violation of the Business Ethics and Conflicts of Interest Policy, and/or other related contracts or agreements (e.g. vendor, consultant, service provider, customer, business partner), and / or applicable laws / regulations. Failure to comply may result in disciplinary action as cited in those documents. Information systems and resources may be monitored to measure compliance.

6.6. IMPLEMENTATION

The UK Chief Financial Officer is responsible for the implementation of this Policy and other related policies and procedures, including the communication and detailed interpretation, monitoring and any disciplinary action in response to an apparent breach of this Policy. The UK IT Manager is responsible for maintaining and reviewing this Policy and for clarifying and resolving any issues arising in relation to it.

6.7. POLICY APPROVAL, COMMUNICATION AND REVIEW

This Policy is subject to review annually, or sooner in response to significant changes in enfinium's business practices or law and regulations to ensure the Policy remains current with enfinium's needs and business objectives.

This Policy is available on enfinium's SharePoint and is required to be read and acknowledged, in the form of electronic sign-off, by all employees, consultants and contractors. Electronic sign-off evidences the policy is read, understood and agreement to comply.

7. BREACHES OF THE POLICY

n/a

8. REVISION HISTORY

Revision	Issue Date	Approval Date	Summary of changes	Approved by:	Next Review
1.0	06/10/20	21/10/20	Initial Issue	IT Manager	06/10/21
1.1	25/05/21	25/05/21	Updating document to enfinium branding	IT Manager	As above