LLW Repository Ltd

LLWR Policy

Policy 01

Issue 5

01/2021

Cyber Security and Information Assurance Policy

This Cyber Security and Information Assurance Policy outlines the approach, methodology and responsibilities for protecting the confidentiality, integrity and availability of LLWR's information and the key information assets of third parties who LLWR provides services to (i.e. the NDA) from all threats whether internal, external, deliberate or accidental. It is the overarching policy for information security and supported by specific technical security, operational security and security management policies.

LLWR recognise that it cannot protect against all threats but this policy will ensure they are detected, assessed and responded to appropriately.

LLWR Commits to:	We will achieve this by:
Clearly **Identify**ing CS&IA Assets, their value and associated risk.	Having an asset management process in place and the relevant registers for Information Assets, physical IT/OT assets and systems. Identifying the business environment and the role with customers and the supply chain Ensuring there is a risk management plan in place for the identification, treatment and escalation of CS&IA risks. Having adequate governance arrangements in place to safeguard the Confidentiality, Integrity and Availability of physical and electronic assets. (appointing a SIRO, IAO and CISO) Ensuring legal and regulatory requirements are fulfilled.
Protecting information assets to ensure delivery of critical services and to limit or contain the impact of a potential cybersecurity event	Implementing the appropriate controls within LLWR and the supply chain, based upon the CS&IA risk assessments. Providing Awareness and Training to all staff based upon their role and responsibilities to ensure a positive security culture is maintained and the appropriate actions are taken when necessary. Ensuring systems are maintained. Having an ongoing audit and assurance programme in place to ensure controls are still effective

Cyber Security and Information Assurance Policy

Detecting the occurrence of a cybersecurity event	Installing protective monitoring solutions where possible to ensure Anomalies and Events are detected Ensuring physical protection and user awareness is robust on systems which have no protective monitoring installed. Implementing Continuous Security Monitoring capabilities to monitor events and verify the effectiveness of protective measures Promoting a positive security reporting culture to ensure all events including near misses are captured and learnt from.
Respond appropriately to a detected cybersecurity incident	Implementing Response plans which include a communication plan. Maintaining and testing the response plans. Ensuring analysis is conducted to ensure effective response and support recovery activities Ensuring lessons learned from previous detection/response activities are documented
Recover from a cyber incident that impairs any capability or service that LLWR relies on.	Ensuring Business Continuity and Disaster Recovery plans are produces, maintained and tested. Implementing Improvements based on lessons learned and reviews

LLW Repository Ltd

LLWR Policy

Policy 01

Issue 5

01/2021

Cyber Security and Information Assurance Policy

LLWR Information Security Policy map