



Date:	Jan.'24	Release:	Publication
Author:	Corp.Sec.		
Owner:	CyberDefenceDynamics		
Document Number:	POLMAN_CSCP		


Revision History

Date of next review

Revision Date	Previous Revision Date	Summary of Changes	Changes Marked
06/01/22	01/07/21	Structural adjustment	
05/01/23	06/01/23	Update of the contract content / structures	
13/01/24	05/01/23	Verification	

Approvals

This document requires the following approvals. A signed copy should be placed in the project files.

Name	Signature	Title	Date of Issue	Version
D.Strudwick		Managing Director	13/01/24	1.04

Purpose

The is an outline policy document (that does not disclose detailed arrangements) but instead, divulges the majority of the outline principles underpinning the security arrangements prevalent in the organisation.

This policy is however, part of a library of commercial management approach including:

- Quality Assurance & Audit
- Safety Criticality in Software Engineering
- Health and Safety
- Ethics and Behaviours
- Environmental and Energy
- Government Security Management
- Special Projects
- Board Management
- Equality Diversity
- Development Policy
- Commercial Contractual Engagement
- Commercial/Professional Insurance

Cyber Security & Contingency Plan Overview

Contents *The Cyber Security and Contingency Planning should encompass at least the following topics.*

Executive Summary.....	3
Basis of CDD Security Policy	4
Scope of Cyber Security Practice.....	5
Access Control	5
Assessment, Authorization, and Monitoring.....	6
Audit and Accountability	6
Awareness and Training	6
Configuration Management	7
Contingency Planning	7
Ethics and Developmental Framework(EDF).....	7
Identification and Authentication.....	8
Incident Response	8
Maintenance	8
Media Protection	9
Personnel Security.....	9
Physical and Environmental Protection	9
Planning	9
Program Management	10
Risk Assessment	10
System Communications Protection and integrity.....	10
System and Services Acquisition.....	11
Redactions.....	11

Cyber Security & Contingency Plan

Executive Summary

CDD operates a bespoke security policy commensurate with the level of risk that the business has to mitigate. Similarly, its reputation as a provider of security is dependent upon it being able to conduct its own cyber security practice efficaciously.

However, guidance in relation to evolving best practice can arise from many sources. As has been attested by HM Government in relation to cyber governance:

Digital technologies now underpin business resilience and cut across so many organisational and strategic areas of the business, from strategy definition and capability building to partner selection or business integration. Executive and non-executive directors therefore need to take greater action to provide stronger governance on technology strategies. Clear leadership, and becoming skilled at governing technology, both capitalising on its opportunity as well as managing risks associated with its adoption and use, is fundamental to doing business today. Management and leaders therefore need to ensure that there is a coherent and practicable strategy which weighs up various interdependencies between competition and risks of security, safety, ethics and reputation. Whether governing of technology issues is done via regular engagement as a recurring agenda item or informal engagement on selected topics, it is critical that executive and non-executive directors develop their understanding and prioritise technology decisions whilst appropriately considering the risks to their business strategy.

What is cyber governance and why is it important?

Cyber governance focuses on a top-down approach to managing and mitigating risks associated with security concerns of the organisation's use of digital technologies. Better governance of cyber security risk is critical to improving the cyber resilience of organisations and better protecting the UK economy and society. Our evidence suggests that a focus on improving the governance of cyber security within an organisation often leads to the fastest improvements in overall cyber resilience. Improving cyber resilience forms part of one of the objectives of the National Cyber Strategy, which sets out the government's commitment to strengthening resilience at national and organisational level to prepare for, respond to and recover from cyber attacks. This approach to cyber resilience is absolutely critical in order to ensure:

- 1. Cyber resilience is embedded within company strategy and integrated across all relevant business processes, not just the IT or technology domains; and*
- 2. Responsibilities for the management of cyber resilience are clear and are embedded across all relevant domains to ensure they are not siloed.*

To govern cyber risk effectively, CDD implements a top-down approach. This requires the directors to take ownership of cyber risk, understand the threats that the organisation faces and assess what action is being taken to manage them.

Cyber Security & Contingency Plan

Basis of CDD Security Policy

CDD has based its security upon NIST SP800-12 which amongst other matters, identifies some 18 control families¹ including:

- Access Control
- Assessment, Authorization, and Monitoring
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Ethics and Development Framework
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Program Management
- Risk Assessment
- System Communications Protection and Integrity
- System and Services Acquisition

There are client specific processes that have been grouped into three categories:

There are 5 practices governing client guidance levels including:

- Specific Mandatory Technical Guidance (SMTG)
- High-Level Outline Approach (HLOA)
- Specific System Level Focus (SSLF)
- Fine Granular/Configuration Controls (FGCC)
- Advanced, Bespoke System Security (ABSS)

There are 5 practices governing commercial activity focus including:

- Risk management
- Cyber Security and Response Strategy
- Personnel Aspects
- Cyber Incident Planning and Response
- Information Assurance and Oversight

Finally there are 7 practices governing technical activities including:

- Identity and Access Management
- Device Security and Configuration
- Email Configuration Practices
- Web Interaction and Public Communication
- Secure Data Transfer
- Encryption and Advanced Security
- Special Information Assurance for Ops Support
- Cyber Security Re-engineering and Modelling

¹ This is not to be confused with NIST SP800-53r5 which contains over 900 specific controls; while such is excellent technical reference material, but well beyond the scope of this guidance document.

Scope of Cyber Security Practice

CDD has structured its own internal security upon families of controls which have arisen from consideration of the following technology based approaches:

- Resilient Inter-domain Traffic Exchange for DDoS Mitigation
- Discrete Logarithm-based Cryptography
- Wireless Network Security
- Firewalls Deployment Policy
- Contingency Planning and Cybersecurity Event Recovery
- Incident Response and Integrating Forensic Technique
- Malware Incident Prevention
- Attribute Based Access Control
- Information Security Continuous Monitoring
- Attribute Considerations for Access Control Systems
- Operational Technology Security
- Industrial Control Systems Security
- Risk Management and Formal Accreditation
- Storage Infrastructure Practices
- Zero Trust Architecture Implementation
- Web-based Operational Security and Site Management (CASB)

A formal (and more detailed) description of these kinds of control families can be found in NIST documentation, however, having been adapted for use in this organisation, the underpinning policy structure and outline approach is available below: (Alphabetical order)

Access Control

Access is the ability to make use of any system resource. Access control is the process of granting or denying specific requests to:

- 1) obtain and use information and related information processing services; and*
- 2) enter specific physical facilities (e.g., Secure client premises, government buildings, military establishments, other RESTRICTED sites).*

System-based access controls are called logical access controls. Logical access controls can prescribe not only who or what (in the case of a process) is to have access to a specific system resource, but also the type of access that is permitted.

These controls may be built into the operating system, incorporated into applications programs or major utilities (e.g., database management systems, communications systems), or implemented through add-on security packages. Logical access controls may be implemented internally to the system being protected or in external devices.

Cyber Security & Contingency Plan

Assessment, Authorization, and Monitoring

Any process of security control assessment involves the testing and/or evaluation of the management, operational, and technical security measures within a system configuration to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Such assessment also assists in determining the efficaciousness of the control implementation and cost-effectiveness of the chosen security approach. Assessment of the security controls is done on a continuous basis to support a near real-time analysis of the organization's current security posture.

CDD undertakes periodically:

- (i) assessment of the security controls in organizational systems to determine if the controls are effective in their application;*
- (ii) verifies the development and implementation plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;*
- (iii) authorizes the operation of organizational systems and any associated system connections; and*
- (iv) tight-monitors the security controls on an ongoing basis to ensure the continued effectiveness of the controls under stress.*

Audit and Accountability

In accordance with CDD's internal Quality Assurance and Audit Procedures (CDD_QAA), appropriate audit trails exist that demonstrate effective control is being exercised. CDD's audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance issues, and flaws in applications.

CDD's approach to audit trails also support regular system operations, a kind of insurance policy, or both. Like insurance, audit trails are maintained but not used unless needed (e.g., after a system outage). As a support for administrative operations, audit trails are used to help system administrators ensure that the system or resources have not been harmed by hackers, insiders, or technical problems. CDD works to

- (i) create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity; and*
- (ii) ensure that the actions of individual system users or threat actors can be uniquely traced and may be held accountable.*

*CDD refers to this style of capability as '5T' activities that effectively **'Transmute'** organisational risk and it is part of a range of such specialist facilities that turn the risk of cyber attack back onto the threat actors.*

Awareness and Training

Making system users aware of their security responsibilities and teaching them correct practices helps change their behaviour. It also supports individual accountability, which is one of the most important ways to improve information security. Without knowing the necessary security measures or how to use them, users cannot be truly accountable for their actions. The purpose of information security awareness, training, and education is to enhance security by:

- (i) raising awareness of the need to protect system resources;*
- (ii) developing skills and knowledge so system users can perform their jobs more securely;*
- and*
- (iii) building in-depth knowledge as needed to design, implement, or operate security*

Cyber Security & Contingency Plan

Therefore CDD ensures that:

- (i) our personnel are made aware of the security risks associated with their activities and of the applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational systems; and
- (ii) personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Configuration Management

CDD establishes and maintains the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the SDLC.

Configuration management consists of determining and documenting the appropriate specific settings for a system, conducting security impact analyses, and managing changes through a project and change control board. It allows an entire system or development to be reviewed, in order to help ensure that a change made on one platform does not adversely impact another. Common security configuration checklists provide recognized, standardized, and established benchmarks that stipulate secure configuration settings for information technology platforms and products. CDD applies this commonality of approach in order to:

- (i) establish and maintain baseline configurations and inventories of organizational systems, including hardware, software, firmware, and documentation throughout the SDLC; and
- (ii) establish and enforce security configuration settings for information technology products employed in organizational systems.

Contingency Planning

CDD's contingency planning of management policy and procedure are used to guide organizational response to a perceived loss of mission capability. A system's contingency plan must determine what may have happened, why, and the most appropriate response. The plan may direct to business continuity operations or a disaster recovery (DR) plan if there was a major issue. The overall DR plan addresses CDD's organization's critical functions operational in the and the events that may lead to disruption. This broader view of CDD contingency planning is based on the organization exercising availability by a number of access routes, thus minimizing the impact of service outage.

CDD has established bespoke mechanisms that:

- (i) establish, maintain, and effectively implement plans for emergency response;
- (ii) backup entire operations; and
- (iii) oversee rapid and seamless recovery of organizational systems to ensure the availability of critical information resources and the continuity of operations in emergency situations.

Ethics and Developmental Framework (EDF)

CDD operates an ethical development framework encompassing Cyber Security practice that is designed to ensure that CDD's special product and service preparation is transparent to the client, ensuring absolute confidence in the technical methods and gives rise to a high-quality and highly secure end-product that is fully tested, properly designed, demonstrably efficient, effectively documented and meaningfully deployed with the intention of meeting the client specification and progressing to training/support and BAU and with the highest levels of cyber security practice.

The special security practices underpinning EDF are beyond the scope of this document and generally classified information.

Cyber Security & Contingency Plan

Identification and Authentication

CDD's identification and authentication and authorization represent critical building blocks for our information security since it is the basis for most types of access control and for establishing user accountability. While access control often requires that the system be able to identify and differentiate between users, user accountability necessitates linking activities on a system to specific individuals and, therefore, requires the system to identify users.

CDD's approach to authentication and identification:

- (i) identify system users,*
- (ii) security processes acting on behalf of users, or devices and*
- (ii) authentication or verification of the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.*

Incident Response

CDD's systems may be subject to a wide range of threat events (form a range of threat groups), from corrupted data files, to viral infestation, to natural disasters. CDD's range of mitigations to such assumed vulnerability might constitute simple restoration from a backed up file. Threat events can also result from crypto-viral malware or other highly targeted malicious code, or perhaps a cyber-intruder. However, swift reciprocative action and effective communications planning in response, usually dramatically reduces any possible adverse impact. CDD has therefore established a largely automated response programme including:

- (i) operational incident handling capability that includes adequate:*
 - preparation*
 - detection*
 - analysis*
 - containment,*
 - communications*
 - recovery*
 - user interactive response activities (SyOPs); and*
- (ii) response mechanisms that:*
 - track progress (i.e. forensic activities)*
 - document technical activities and deployment of countermeasures*
 - report preparation of (aggressive) incidents and progression*
 - prepare legally admissible evidence (and provide it to appropriate official bodies)*
 - establish 'lessons learnt' reports for future review and process improvement*

Maintenance

CDD has established procedures for the scheduled regular maintenance of organizational systems, over and above (or correctively beyond) manufacturer specifications. This avoids system failures or generation of error conditions in sensitive, high performance apparatus and eases the process of systems verification, but removing a possible source of error condition. Consequently, CDD specifically undertakes to:

- (i) perform periodic and timely maintenance on organizational systems; and*
- (ii) ensure that equipment is properly ventilated, by cleaning away dust/detritus in filters*
- (iv) provide effective controls on the tools, techniques, mechanisms, and personnel whom conduct such system maintenance.*

Cyber Security & Contingency Plan

Media Protection

CDD uses external media in the form of:

- High density USB drives (up to 8TB)*
- Compact Disk Read/Write (very long term storage(VLTS))*
- Encrypted Cloud Storage*
- Paper (i.e. Printed information)*

When in use, media is locked away in approved storage containers (i.e. data safes or government approved D-Type Manifold safes). CDD specifically undertakes to:

- (i) protect system media (both paper and digital);*
- (ii) limit unauthorised access to data/information; and*
- (iii) sanitize or destroy system controlled media before disposal or release for re-utilization;*
- (iv) shred/incinerate redundant papers as appropriate for their classification.*

Personnel Security

CDD's professional reputation and status could be adversely affected by ill-considered actions of its personnel. CDD routinely handles much extremely sensitive, confidential, or proprietary information, the disclosure of which can destroy a client organization's reputation or damage the entity financially.

Therefore CDD ensures that:

- (i) individuals occupying positions of responsibility meet established security criteria for those positions;*
- (ii) organizational information and systems are protected during and after personnel actions such as transferal; and*
- (iii) retraining and guidance takes place following any accidental failure of compliance with SyOPs*

Physical and Environmental Protection

CDD's physical and environmental controls cover three broad areas:

- a. The physical facility being the building housing the system and network components.*
- b. The facility's general geographic operating location*
- c. Supporting facilities are those services (both technical and human) that maintain the operation of the system.*

CDD makes appropriate arrangements to:

- (i) limit physical access to systems, equipment, and the respective operating environments to authorized individuals;*
- (ii) protect the physical support infrastructure for systems;*
- (iii) provide supporting utilities and apparatus for systems (e.g. aircon);*
- (iv) disruption of the possible emanation of signals from electronic apparatus (TEMPEST)*
- (v) protect systems against environmental hazards (e.g. power fluctuations); and*
- (vi) provide appropriate environmental controls (e.g. Strong locks & video cameras)*

Planning

CDD undertakes proper planning of security approach to systems commensurate with the risk associated with the operation of the system. This tends to increase productivity and professional performance by avoiding the distractions that arise from poor security measures, as well as ensuring CDD's information security goals are achieved.

Cyber Security & Contingency Plan

CDD then takes care to implement, document, and periodically review/update detailed security plans for all the critical organizational systems. Such audit assures that the most appropriate controls have been engineered as the risk changes, as well as ensuring the most appropriate SyOPS properly reflect the necessary access for specific system(s).

Program Management

CDD's approach to Delivery Program Management level security controls include:

- i) Information security program plan,*
- ii) Information security resources,*
- iii) Technical milestone process,*
- iv) System inventory,*
- v) Enterprise security architecture,*
- vi) Risk management strategy,*
- vii) Threat awareness and technical hunting program.*

Risk Assessment

CDD's outline approach to security risk includes regular re-assessment of /to organisational:

- (i) operations (e.g., mission, functions, image, reputation),*
- (ii) business systems, assets, and individuals*
- (iii) process and systems and the associated;*
 - processing,*
 - storage, or*
 - transmission of organizational/client information.*

System Communications Protection and integrity

CDD takes steps to carefully monitor, control and protect organizational communications at the external boundaries and key internal boundaries of the systems, especially that relating to:

- a) architectural designs,*
- b) software development techniques, and*
- c) advanced research approach*

- and all processes that promote effective information security within its own systems, while at all times:

- (i) identifying, reporting and correcting information and system flaws in a timely manner;*
- (ii) providing protective process/defence from malicious code at appropriate locations within organizational systems; and*
- (iii) gathering and analysing logs in order to monitoring system security alerts and advisories and respond appropriately.*

Cyber Security & Contingency Plan

System and Services Acquisition

CDD is fully cognizant that security-relevant events and analyses occur during a system's life which begins with the organization acquiring the necessary tools and services. The effective integration of CDD's security requirements into enterprise architecture also helps to ensure that important security considerations are addressed early in the SDLC and that those considerations are directly related to the organizational mission/business processes.

CDD's approach to the protection of its communications by:

- (i) allocation of sufficient resources to adequately protect critical organizational systems;*
- (ii) employ SDLC processes that incorporate information security considerations (such as appropriate strength encryption);*
- (iii) employ software usage and installation restrictions; and*
- (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization (e.g. Suitable protections for our systems/data in transit).*

Redactions

**DETAILS OF THE FOLLOWING PROCESSES HAVE
BEEN REDACTED FROM PUBLIC DOCUMENTATION
FOR REASONS OF CLIENT CONFIDENTIALITY**

Guidance Material including:

- Specific Mandatory Technical Guidance (SMTG)
- High-Level Outline Approach (HLOA)
- Specific System Level Focus (SSLF)
- Fine Granular/Configuration Controls (FGCC)
- Advanced, Bespoke System Security (ABSS)

Commercial Activity Focus including:

- Risk management
- Cyber Security and Response Strategy
- Personnel Aspects
- Cyber Incident Planning and Response
- Information Assurance and Oversight

Client Specific Technical Activity including:

- Identity and Access Management
- Device Security and Configuration
- Email Configuration Practices
- Web Interaction and Public Communication
- Secure Data Transfer
- Encryption and Advanced Security
- Special Information Assurance for Ops Support
- Cyber Security Re-engineering and Modelling