Nexus Select Malls

Cybersecurity Framework Baseline

Version 1.0

Document Information	
Title	Cybersecurity Framework Baseline
Version	1.0
Effective Date	
Policy Owner	InfoSec Team
Policy Reviewed By	Head – IT Security & Ops
Policy Approved By	CTO
Review Period	Annually

Revision History

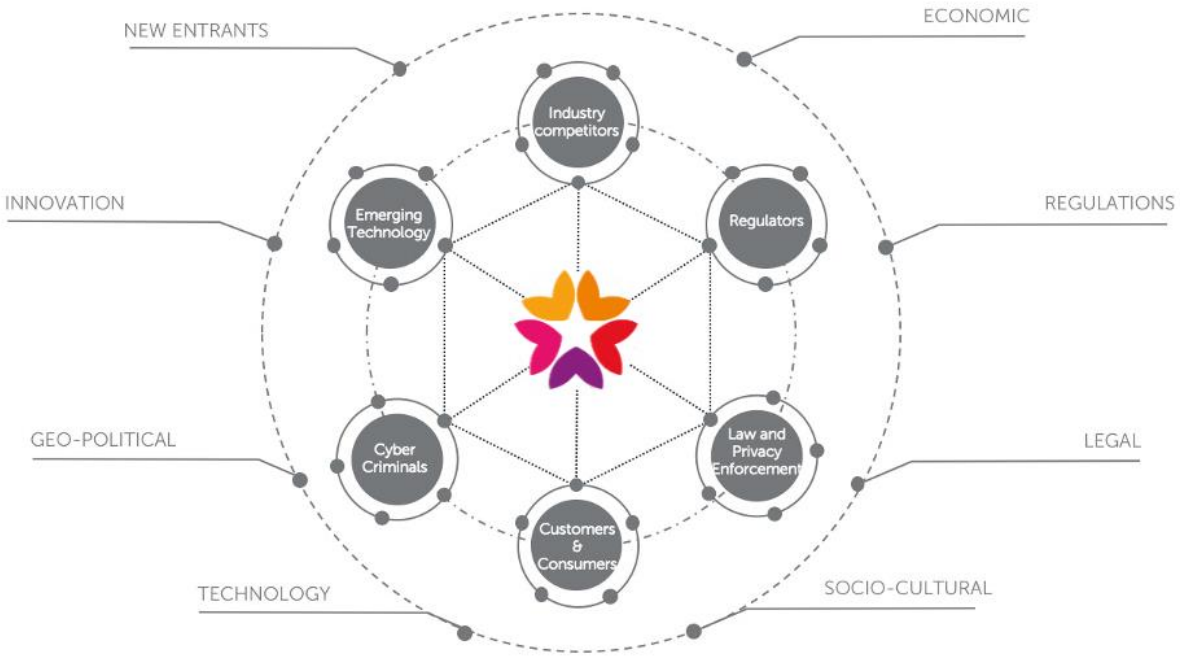
Version	Date Created	Author	Change Description
1.0	August 2024	InfoSec Team	Cybersecurity Baseline Framework

Table of Contents

1. Preface

The purpose of cyber security is to ensure that information can be used when required in the conduct of business with the confidence that it is accurate and complete, and that it is adequately protected from misuse, unauthorised disclosure, damage or loss.

Nexus Select Malls, while primarily a physical retail entity, manages significant digital and cyber risk due to its online presence and digital infrastructures. As a digital business, Nexus Select Malls (and its subsidiaries) operates in an increasingly complex operating environment, managing cyber risk across organisational, technical and geographic boundaries. Threats can occur from a variety of points within the eco-system in which Nexus Select Mall operates.



2. Purpose

The purpose of this document is to define the cybersecurity baseline standards which must be applied to maintain the confidentiality, integrity and availability of the information and IT Assets supporting the business processes of Nexus Select Malls.
This policy is an **operational** policy. This means that all aspects of the policy are mandatory and must be adhered to by all staff.

This policy sets out the minimum acceptable security **objectives** that are designed to help Nexus Select Malls meet its risk appetite. As such, this policy does not define **how** an objective should be achieved, since Nexus Select Malls operates in a complex technical landscape and security objectives may be achievable by a variety of means. Operational standards may provide guidance as to the preferred method of meeting a security objective defined within this policy.

3. Scope

This policy covers all technology assets of Nexus Select Mall. This policy also applies to all Nexus Select Malls employees and contractors (including consultants and third-party personnel) who are directly or indirectly employed by Nexus Select Malls (henceforth referred to as 'users') and authorized to access and use Nexus Select Malls information assets and subsidiaries or any entity conducting work on behalf of Nexus Select Malls.

4. Framework and Definitions

Nexus Select Malls has established its cybersecurity best practices in alignment with the NIST CSF[1] 2.0 Framework. As a listed entity, the framework also overlaps with SEBI's CSCRF[2] requirements. Additionally, all necessary compliance enhancements are incorporated through annual reviews and recommendations from external cybersecurity experts to ensure continuous improvement.

NIST Cybersecurity Framework

For the purpose of this policy, the terms and definitions given in NIST Cybersecurity Framework v2.0 apply.

The NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework, or CSF) was originally published in February 2014 in response to Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which called for the development of a voluntary framework to help organizations improve the cybersecurity, risk management, and resilience of their systems. NIST conferred with a broad range of partners from government, industry, and academia for over a year to build a consensus-based set of sound guidelines and practices.

[1] National Institute of Standards and Technology Cybersecurity Framework
[2] SEBI's Cyber Security and Cyber Resilience Framework

The Cybersecurity Enhancement Act of 2014 reinforced the legitimacy and authority of the CSF by codifying it and its voluntary adoption into law, until the Presidential Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" signed on May 11, 2017, mandated the use of CSF for all U.S. federal entities.

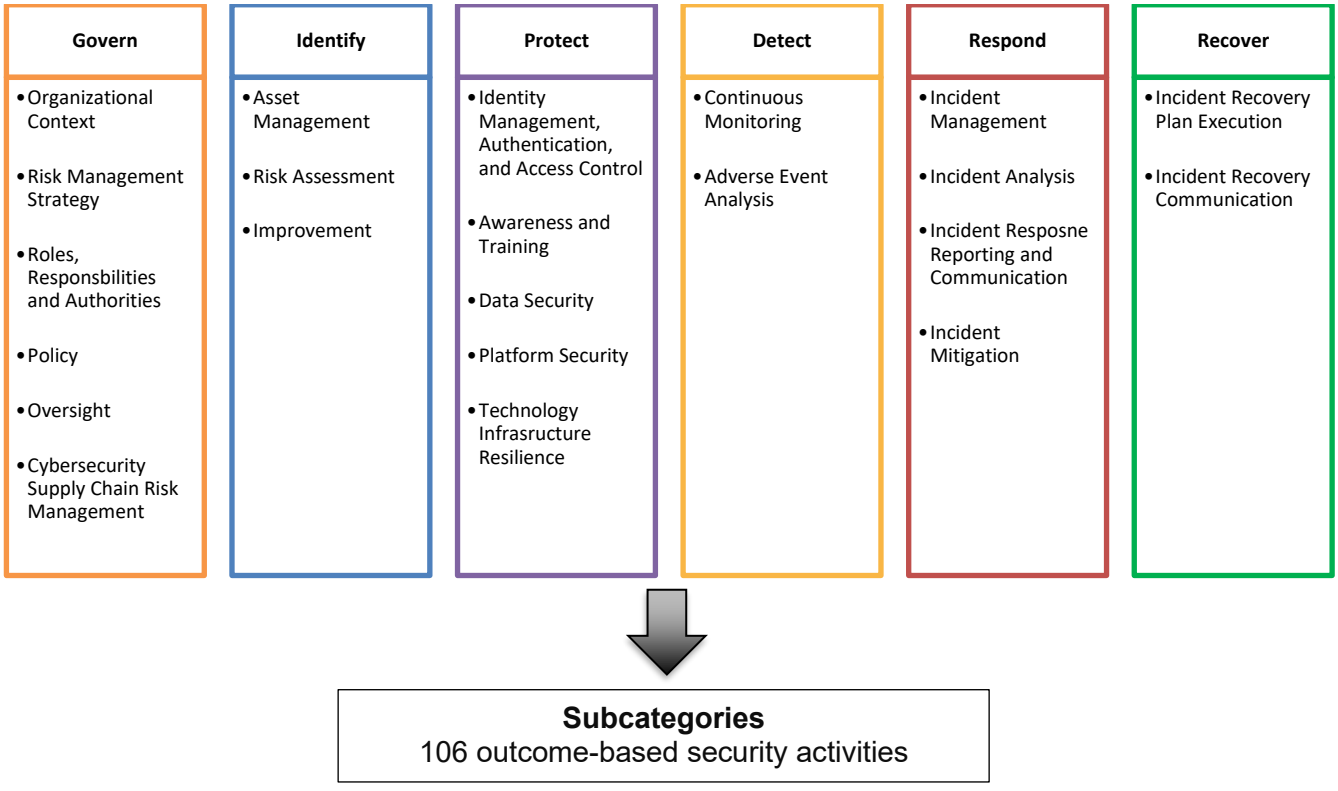
While intended for adoption by the critical infrastructure sector, the foundational set of cybersecurity disciplines comprising the CSF have been supported by government and industry as a recommended baseline for use by any organization, regardless of its sector or size. Industry is increasingly referencing the CSF as a de facto cybersecurity standard.

International adoption

Outside of the U.S., many countries have leveraged the NIST CSF for commercial and public sector use. Italy was one of the first international adopters of the NIST CSF and developed a national cybersecurity strategy against the five functions. In June 2018, the UK aligned its Minimum Cyber Security Standard- mandatory for all government departments- to the five functions.

Additionally, Israel and Japan localized the NIST CSF into their respective languages with Israel creating a cyber defense methodology based on its own adaptation of the NIST CSF. Uruguay performed a mapping of the CSF to ISO standards to strengthen connections to international frameworks. Switzerland, Scotland, Ireland, and Bermuda are also among the list of countries that are using the NIST CSF to improve cybersecurity and resiliency across their public and commercial sector organizations.

Core Functions



5. Related Policies, Guidelines and/or Procedure

The following policies and guidelines should be read in conjunction with this Policy.

- Using Technology Safely
- Looking after people's information
- Nexus Select Malls - Information Handling Policy
- ISMS Policy

6. Nexus Select Mall Cybersecurity Policy

How to read this policy

Security objectives defined in this policy are assigned to 3 roles – All Staff, Operations Staff and Technical Staff. Objectives that must be met are indicated by [**X**]. This means all personnel as defined in table 6.1 must meet the objective.

Objectives accountable to the role of **Operations Staff** or **Technical Staff** are **ADDITIONAL** accountabilities to **All Staff**.

In practice, this means that Product and Technical staff have greater accountability under this policy due to the nature of their role and the fact they operate additional controls that are designed to meet objectives outlined within this policy.

Roles

This policy has been divided between accountable roles within Nexus Select Malls. For the purposes of this policy, accountable roles have been highly simplified to ensure that staff have clear understanding of their accountabilities outlined in the policy.

Table 6.1

Role (as outlined in this policy)	**Definition** (who this applies to)	**Examples** (note – not all Nexus Select Malls roles)
All Staff	Unless otherwise defined, all staff relates to any personnel working for or with Nexus Select Malls who have been authorised to access Nexus Select Mall's IT Assets.	Sales, marketing, finance, people & culture etc. i.e. roles not directly involved with defining, developing or creating products for technology.

Operations Staff	This role applies to personnel involved in managing and supporting the day-to-day functions of the mall properties, including roles responsible for the delivery and execution of operational activities.	This category includes roles such as Facility Managers, Operations Managers, and Maintenance Teams.
Technical Staff	This role applies to personnel involved with building, maintaining and operating technology including administration duties, i.e. non-functional requirements.	Engineering, Operations, Technology staff, Third party vendors for technical support.

GOVERN

Organizational Context (GV.OC)

By establishing a comprehensive understanding of our organizational structure, roles, responsibilities, and relationships, we can effectively govern and manage our cybersecurity efforts. This ensures alignment with our strategic objectives, compliance requirements, and risk management strategies, allowing us to maintain a security posture that supports our overall mission and risk tolerance.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Ensure compliance with the governance structure and;			
- Develop strategic objectives, compliance requirements and risk management strategy	X		
- Review and understand the organization's mission statement and core objectives	X		
- Actively address stakeholder concerns and adjust cybersecurity practices as necessary		X	X
- Identify and review applicable legal, regulatory, and contractual requirements related to cybersecurity		X	X
- Enforce implementation of policies and procedures to meet legal and regulatory requirements		X	X

- Communicate critical objectives and capabilities to external stakeholders to ensure transparency and alignment		X	X
- Measure the organization's cybersecurity capabilities against industry standards and benchmarks		X	X
- Promote improvements to enhance cybersecurity outcomes and capabilities		X	X

Risk Management Strategy (GV.RM):

By developing and implementing a robust risk management strategy, we ensure that cybersecurity risks are identified, assessed, and mitigated in alignment with our organizational risk appetite. This strategic approach enables us to prioritize resources, make informed decisions, and maintain resilience against potential threats, thereby supporting the overall mission and strategic objectives of our organization.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Adhere to the Nexus Select Malls Risk Management Framework including:			
- Maintaining a risk register		X	X
- Reporting security risks that could be outside Nexus Select Malls' risk appetite		X	X
- Implement or comply with security recommendations that are required to reduce, mitigate or manage a risk to an acceptable level			X
- Establishing and maintaining risk appetite and risk tolerance		X	X
- Collaborate with other departments to ensure that cybersecurity risks are considered alongside other types of risks in enterprise risk management processes		X	X
- Develop and review strategic directions and response options for managing cybersecurity risks, including mitigation, acceptance, transfer, or avoidance		X	X

- Implement mechanisms for effective communication and coordination regarding cybersecurity risks		X	X
- Develop standardized methodology for calculating, documenting, categorizing, and prioritizing cybersecurity risks		X	X
- Identify and characterize strategic opportunities (positive risks) that could benefit the organization		X	X

Roles, Responsibilities, and Authorities (GV.RR)

By clearly defining and communicating the roles, responsibilities, and authorities within our organization, we ensure that all personnel understand their specific duties in maintaining and enhancing our cybersecurity posture. This clarity promotes accountability, enhances coordination, and ensures that security measures are effectively implemented and maintained, thereby supporting our overall governance and risk management framework.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Develop Roles and Responsibilities to:			
- oversee cybersecurity risks and fostering a risk-aware culture		X	X
- Foster a culture that values risk awareness, ethical behaviour, and continuous improvement in cybersecurity practices		X	X
- Establish risk management committee		X	X
- Allocate sufficient resources to support effective implementation and management of cybersecurity practices		X	X
- Incorporate cybersecurity in HR practices such as recruitment, training, performance evaluations, and role assignments	X		

Policy (GV.PO)

By establishing comprehensive cybersecurity policies, we set clear guidelines and expectations for managing and protecting our information assets. These policies provide a foundation for consistent and effective security practices across the organization, ensuring compliance with legal, regulatory, and industry standards. Through well-defined policies, we promote a culture of security awareness and responsibility, supporting our overall governance framework and strategic objectives.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
ensure compliance with legal, regulatory, and industry standards, this includes;			
- Develop cybersecurity policies		X	X
- Regularly review and update cybersecurity policies		X	X

Oversight (GV.OV)

By implementing effective oversight mechanisms, we ensure that our cybersecurity strategies and practices are regularly monitored, evaluated, and improved. This oversight includes internal audits, management reviews, and independent assessments, which provide assurance that our security measures are functioning as intended and align with our organizational goals. Through diligent oversight, we maintain accountability, enhance transparency, and continuously refine our cybersecurity posture to address evolving threats and challenges.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
manage cyber supply chain risk with suppliers and third party partners, including;			
- Define and track key performance indicators (KPIs) and metrics to measure the effectiveness of the cybersecurity risk management efforts		X	
- Develop a formal procedure for adjusting the risk strategy based on assessment findings		X	X
- Regularly review and analyse risk assessment findings to determine effectiveness and areas for improvement		X	

Cybersecurity Supply Chain Risk Management (GV.SC)

we ensure that all external dependencies, including vendors and service providers, adhere to our security standards. This proactive approach involves assessing and mitigating risks associated with third-party products and services, ensuring that our supply chain does not introduce vulnerabilities into our environment. By managing these risks, we protect our assets and maintain the integrity and resilience of our overall cybersecurity framework.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
manage cyber supply chain risk with suppliers and third party partners, including;			
- adherence to Nexus Select Malls' procurement policies, process and procedures		X	X
- performing enhanced due diligence where criteria is met		X	X
- designing contracts that align to Nexus Select Malls' security risk appetite			
- routine assessment of critical suppliers* to evaluate the are meeting their contractual obligations			
- routine assessment of response and recovery plans for critical suppliers*			

IDENTIFY

Asset Management (ID.AM)

By knowing (and having visibility) into where all our people, devices and systems are, we're able to better determine our security posture and identify any exposures to security threats which may not be in line with our security risk appetite.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
identify all devices, systems, services and create an inventory of associated assets, this includes (but is not limited to):			
- Physical devices.		X	X
- Software, platforms and applications		X	X
develop and maintain supporting documentation, which includes:			

- information on the business criticality of these devices, systems or services		X	X
- documenting the flow of information (e.g. A dataflow diagram) which shows connections between Nexus Select Mall's internal and external systems (e.g. AWS)		X	X

Risk Assessment (ID.RA)

Cybersecurity threats are one of many risks that could have a financial, reputational, legal, people or business continuity impact to Nexus Select Malls. So, we need to make sure that any actions we take (that may increase our exposure to these threats) is carefully considered and discussed with the right level of decision makers.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Conduct a Risk Assessment when Nexus Mall's information is being handled, stored or transmitted across networks or with third parties. Risk assessments will be used to:			
- identify threats (internal / external)		X	X
- identify asset vulnerabilities		X	X
- understand business impacts and the likelihood of them occurring			X
- Identify cyber threat intelligence from information sharing forums and sources			X
- Analyse and respond to vulnerabilities		X	X
- Identify critical suppliers prior to acquisition		X	X

Improvement (ID.IM)

Continuous improvement is crucial for maintaining an effective cybersecurity posture. By regularly reviewing and refining our security measures, we can adapt to emerging threats and evolving business needs. This ongoing process ensures that our cybersecurity practices remain robust and relevant, minimizing potential impacts on our financial, reputational, legal, people, and business continuity. Any identified gaps or areas for enhancement are carefully analyzed and addressed to uphold our commitment to resilience and security.

Policy Objective	Accountable Role

Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Conduct Regular Improvement Activities to Enhance Nexus Mall's Cybersecurity Posture. Improvement activities will focus on:			
- Regularly review and update cybersecurity policies and procedures			X
- Assess the effectiveness of security measures and identify areas for improvement		X	X
- Implement recommendations from security audits and assessments			X
- Monitor and evaluate the effectiveness of implemented improvements		X	X
- Ensure continuous education and training on emerging threats and new security trends	X	X	
- Engage in regular security drills and incident response exercises			X
- Report and document all improvements and their impact on the security posture		X	X

PROTECT

Identity Management, Authentication, and Access Control (PR.AA)

Your Nexus Select Mall identity (just like your personal identity) is one of your most valuable assets.

If your Nexus Select Mall's account is compromised, your identity can be used to gain unauthorised access to valuable Nexus Select Mall's information. However, if you only have the access you need, in the worst case scenario, any malicious activity is confined to the boundary of your access.

Policy Objective	**Accountable Role**		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
manage identities and credentials for systems where information is stored, used or transmitted from, including;			
- authorised devices and personnel			X
- use unique identifiers		X	X

Policy Objective	Accountable Role		
- physical access			X
- remote access		X	X
when building, changing or maintaining access and authorisation systems;			
- authenticate users commensurate with the risk of the transaction (i.e. multi-factor for high-risk transactions or access to sensitive data)			X
- use the principle of least privilege (need-to-know) and incorporate segregation of duties when defining roles		X	X
- define and manage ownership of shared accounts (e.g. system accounts)			
- ensure access remains assigned on a business-need-only basis			

Awareness and Training (PR.AT)

The wicked people of the internet are always learning. Just like them, we must maintain our vigilance and make sure we're aware of the new ways in which they wish to take advantage of our Nexus Select Mall's identities. This helps us prepare for situations where the worst happens and what we can do to protect ourselves and Nexus Select Mall.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
be informed and trained in their security roles and responsibilities including:			
- complete mandatory security training / applicable policies	X		
- report security incidents including suspicious emails	X		

Data Security (PR.DS)

Nexus Select Mall has a no tolerance for the loss of consumer and customer data and has designed its security and privacy programs around this tolerance level.

Security controls for our products must also be designed with this in mind and there are a number of security tools which provide the acceptable levels of control required for listed entity, which is subjected to the Privacy Act.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
manage and protect Nexus Select Mall's Data Assets;			
- throughout their lifecycle (including creation, transfer and destruction)	X		
- where appropriate, incorporating integrity checking mechanisms to verify authenticity and prevent tampering		X	X
- protecting when in transit (e.g. by using secure tunnels)		X	X
- protecting when at rest (e.g. by using strong encryption)		X	X
- protecting when in use, against unauthorised access (e.g. by using strong authentication)	X		
- securely destroyed when no longer required		X	X
- retain data only when there is a valid business reason to do so, and in compliance with Privacy requirements	X		
- creating, protecting, maintaining and testing backup			X

Platform Security (PR.PS)

The digital landscape is constantly evolving, and so are the tactics of cyber adversaries. To stay ahead, we must ensure that our Nexus Select Mall's platforms are fortified against threats. By securing our applications, systems, and infrastructure, we protect our sensitive data and maintain trust with our users. Vigilant platform security helps us prepare for and defend against attacks, ensuring the integrity and resilience of Nexus Select Mall's digital presence.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Ensure Robust Platform Security for Nexus Mall's Systems and Applications. Platform security measures will focus on:			

Policy Objective	Accountable Role		
- Implement and maintain robust security controls and configurations for all platforms and systems	X		
- Regularly review and update security configurations of application, system and infrastructure		X	X
- Apply necessary patches and updates in software and systems			X
- Generate Logs and monitor platform activity for unusual or unauthorized activity			X
- Ensure secure coding practices are followed during development and deployment		X	X
- Prevent installation and execution of unauthorised software			X

Technology Infrastructure Resilience (PR.IR)

Just as a backup generator ensures that a power outage doesn't cripple a hospital's operations, we need to ensure our technology infrastructure is resilient. By implementing strong resilience measures, we protect our systems from disruptions and ensure that if an incident occurs, we can quickly recover and fortify our defenses. This proactive approach enables us to identify and prevent future issues, and maintain the continuity and reliability of our technology infrastructure.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Establish robust technology infrastructure resilience which includes -			
- Protecting network from unauthorised logical access by implementing; - Access Controls - RBAC and Least privilege - Network Segmentation – DMZ and VLANs - IDS IPS			X
- Protecting from environmental threats - Physical and environmental security - Disaster recovery plan		X	X

Policy Objective	Accountable Role		
- Implement redundancy and failover mechanisms to ensure continuous operation			X
- Capacity planning, monitoring resource utilization and plan for infrastructure upgrades			X

DETECT

Continuous Monitoring (DE.CM)

The wicked people who target Nexus Select Mall work around the clock with automated tools and alerting (just like us) so we need to ensure we have tooling which alerts us to any odd activity around the clock.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Establish continuous monitoring to detect anomalies, indicators of compromise, and other potentially adverse events			
Network Monitoring - Deploy network monitoring tools - Analyze network traffic - Set up alerts			X
Physical Environment Monitoring - Implement environmental sensors and surveillance system - Monitor physical access		X	
Personnel Activity and Technology Usage Monitoring - Deploy EDR - Implement UEBA to monitor user behaviour - Maintain user activity logs			X
External Service Provider Activities Monitoring - Review service provider logs - Conduct third-party audits to review contractual clauses, security standards and practices		X	X

Policy Objective	Accountable Role		
- Implement SLA			
Computing Hardware, Software, and Runtime Environments Monitoring - Deploy system monitoring tools to monitor health and performance of hardware, software and runtime environments			X

Adverse Event Analysis (DE.AE)

We must thoroughly analyze adverse events to understand their origins and impact. By meticulously examining these incidents, we gain insights into vulnerabilities and shortcomings, allowing us to refine our security measures and strengthen our defenses. This analytical approach helps us learn from setbacks, improve our protective strategies, and enhance the overall resilience of our systems.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Establish adverse event analysis which includes;			
Analyzing Adverse Events to Understand Associated Activities - reviewing logs, network traffic, and user activities - map out event chains to understand its broader impact and potential connections			X
Correlating Information from Multiple Sources - Deploy Security information and event management (SIEM) tool - Gather IoCs from threat intel feeds, security logs and incident reports - Analyze correlated data by comparing against internal logs and data to identify potential compromises within the organization.			X
Understanding Impact and Scope of Adverse Events - Assess potential impact of the adverse event - Determine affected assets - Estimate the scope and document findings			X

Policy Objective	Accountable Role		
Providing Information to Authorized Staff and Tools - Disseminate Information and communicate findings - Ensure information is available on incident response tools and platforms for coordination and response			X
Integrating Cyber Threat Intelligence and Contextual Information - Use threat intelligence feeds from external sources - Enhance adverse event analysis using contextual information			X
Declaring Incidents Based on Defined Criteria - Develop and document criteria for declaring an incident based on the severity, impact, and scope of adverse events - Initiate incident response based pn defined criteria and activate incident response plan - Record the declaration and rationale to support incident management and reporting		X	X

RESPOND

Incident Management (RS.MA)

If the worst happens, it's important to have a plan. Nexus Select Mall has a Business Continuity & Resilience Framework which helps teams design their own incident response plan.

Well designed, tested and practiced plans means the actual business impact of incidents are minimised and teams can get back to doing what they do best, quicker.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Ensure incident management includes -			
- Coordination with Relevant Third Parties and establishing communication channels	X		
- Incident reports are triaged - Incident reports are validated		X	X

Policy Objective	Accountable Role		
- Incidents are categorised - Incidents are prioritized			X
- Incidents are escalated or elevated as needed			X
- Define recovery criteria	X	X	X

Incident Analysis (RS.AN)

Incident Analysis is crucial for understanding and addressing security breaches. By systematically examining each incident, we identify the root causes, assess the impact, and evaluate our response effectiveness investigation are recorded, and the records' integrity and provenance are preserved. An incident's magnitude is estimated and validated This process enables us to refine our incident response strategies, strengthen our defenses, and enhance our overall preparedness for future threats.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Ensure incident analysis includes -			
- Root cause analysis		X	X
- Documenting investigation actions and maintaining logs - Preserve Integrity and Provenance of investigation records		X	X
- Use forensic tools to gather metadata and ensure its integrity and provenance is preserved			X
- Estimate magnitude of an incident - Review and validate the magnitude			X

Incident Response Reporting and Communication (RS.CO)

Just as a clear and timely broadcast keeps passengers informed during an emergency evacuation, effective incident response reporting and communication ensures internal and external stakeholders are promptly and accurately updated during a security incident. By maintaining transparent and efficient communication channels, we ensure that critical information is shared, decisions are well-informed, and responses are coordinated. This approach helps manage the incident effectively, maintain trust, and facilitate a swift recovery.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Execute response plans during or after an event, for which:			
- information is shared consistent with response plans	X		
- coordination with stakeholders is consistent with response plans		X	X
- voluntary information sharing occurs with designated internal and external stakeholders to achieve broader cybersecurity situational awareness		X	X

Incident Mitigation (RS.MI)

Our approach involves promptly neutralizing and controlling security breaches to minimize their impact. By implementing targeted actions to contain, eradicate, and recover from incidents, we reduce the threat's potential harm and restore normal operations as quickly as possible. This proactive approach ensures that our response is effective, and vulnerabilities are addressed to prevent recurrence.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Mitigate incidents, ensuring:			
- incidents are contained	X		
- Incidents are eradicated		X	X

RECOVER

Incident Recovery Plan Execution (RC.RP)

Our incident recovery plan involves systematically restoring operations and minimizing disruption following a security breach. By following a detailed recovery plan, we efficiently address the aftermath of an incident, restore systems and data, and resume regular activities while ensuring that lessons learned are applied to strengthen future resilience. This approach guarantees that we recover swiftly and effectively, reducing the impact on our organization.

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Operations Staff**	**Technical Staff**
Ensure recovery plan execution includes			
- Integration with incident response plan - Activation of recovery plan upon incident resolution	X		
- Identifying necessary recovery actions based on the impact and scope of the incident		X	X
- Prioritizing recovery actions to address the most critical systems and services first		X	
- Backup integrity verification using tools			X
- Validation of restoration process		X	X
- Evaluating impact of recovery actions		X	X
- Integrating risk management practices into recovery process		X	X
- Establishing post incident norms		X	
- Verify integrity of restored systems - Operating status is confirmed DE		X	X
- Formal declaration of recovery completion based on predefined criteria		X	X
- incident-related documentation is completed, including recovery actions, outcomes, and lessons learned and reports are reviewed by stakeholders		X	X

Incident Recovery Communications (RC.CO)

Clear and consistent updates are crucial during a disaster recovery to keep affected parties informed, we ensure that restoration activities are coordinated with internal and external parties

Policy Objective	Accountable Role		
Accountable roles must;	**All Staff**	**Product Staff**	**Technical Staff**

Policy Objective	Accountable Role		
Carry out recovery communication, which includes;			
- Sharing of recovery status updates to designated internal and external stakeholders	X		
- Public communication strategy		X	X
- Approved communication channels such as press releases, official websites, social media and news outlets		X	

7. Reference

Version	Document
-	Nexus Select Malls – ISMS Policy
	Using Technology Safely
	Looking after people's information
	Nexus Select Malls - Information Handling Policy
	Nexus Select Malls - Risk Management Framework