Document Title	Cyber Security Policy
Document Code	ITPOLCYBS01
Date of Release	12-Feb-2023
Document Revision No	1
Document Owner	Vikram Vij

Document Prepared by:

S. No	Name	E-Mail
1	Arun Singh	Arun.singh@maxestates.in

Document Approvers:

S.No	Approver	Approver E-Mail Contact
1	Vikram Vij	**Vikram.vij@maxestates.in**

Document Change History

Version No	Revision Date	Nature of Change	Date Approved
1	05-Feb-2023	Initial Document	05-Feb-2023

Title	Cyber Security Policy
Version	Version 1.0
Date	05-Feb-2023
Language	English
Department Responsibility	Information Technology Department – Max Estates Ltd.
Responsibility	All Departments
Developed by:	Max Estates Ltd. (MEL)
Subject	Security
Approval Date	05-Feb
Purpose of Document	The purpose of this document is to define the policies and standards which must be applied to maintain the confidentiality, integrity and availability of the information and IT assets supporting the business processes of MEL.
Distribution of Document	All Departments

Overview

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, unauthorized disclosure, damage, or loss.

As a digital business, MEL (and its subsidiaries) operates in an increasingly complex operating environment, managing cyber risk across organizational, technical, and geographic boundaries. Threats can occur from a variety of points within the eco-system in which MEL operates.
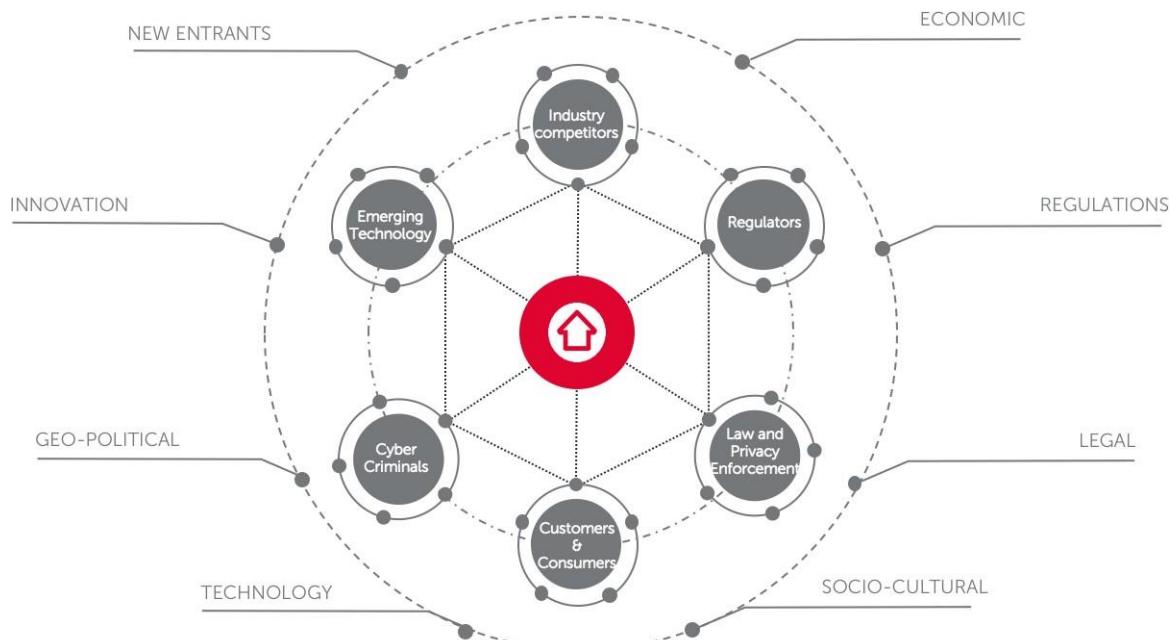
Purpose & Scope

Purpose

The purpose of this document is to define the policies and standards which must be applied to maintain the confidentiality, integrity and availability of the information and IT assets supporting the business processes of MEL.

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 MEL meet its risk appetite. As such, this policy does not define **how** an objective should be achieved, since MEL 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.

Scope

Organization and applicability

This Policy covers all IT assets within MEL. IT assets include all information, data, software, hardware and communications equipment and networks owned or operated by or for MEL.

Assets and Services

MEL's IT assets may be owned, leased, hired, developed in-house, or purchased, and include all computing facilities along with interconnecting networks. The MEL Cyber Security Policy covers all assets and services which are operated, contracted and/or outsourced by MEL.

Personnel

This Policy applies to all **Personnel** working for, or with, MEL who have been authorized to access MEL's IT Assets.

Personnel are defined as all management, employees, contractors, consultants, and parties engaged (including contract personnel) by or for MEL.

However, it excludes Brokers, Customers and Consumers (e.g. people who advertise property, place ads or are typical site users) of MEL.

Local differences

This Policy covers all of MEL companies. Some business areas may choose to create **additional** cyber security policy documentation to reflect their particular business requirements; if so, such policies will be viewed as subordinate / complementary to this MEL Cyber Security Policy.

Definitions & Descriptions

Personal Information is as defined by the Privacy Act 1988 as:

"Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

1. whether the information or opinion is true or not; and

2. whether the information or opinion is recorded in a material form or not." Or as otherwise defined in *The Way We Do Things: Looking After People's Information.*

MEL Security Policy

1.1 How to Read This Policy

Security objectives defined in this policy are assigned to three roles – All Staff, Product Staff and Technical Staff. Objectives that must be met are indicated by [X]. This means all personnel as defined in section 1.3 must meet the objective.

Objectives accountable to the role of Product Staff or Technical Staff are additional accountabilities to all the 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.

1.2 Roles

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

Role (As outlined in this policy)	Definition (Who this applies to)	Examples (Note – not all MEL roles)
All Staff	Unless otherwise defined, all staff relates to any **personnel** working for or with MEL who have been authorized to access MEL's IT assets.	Leadership Teams, Managers, Sales, Marketing, Finance, People & Culture etc. (I.e., Roles not directly involved with defining, developing, or creating products for technology.)
Product Staff	This role applies to any **personnel** involved with defining, developing, and delivering products and services, i.e., functional requirements.	Product Managers, Business Analysts, Delivery Leads, Head of Product.
Technical Staff	This role applies to **personnel** involved with building, maintaining and operating technology including administration duties, i.e., non- functional requirements.	IT Leadership Teams, Developers, Engineering, Operations, Security, Enterprise Technology & Platforms.

1.3 The NIST Cybersecurity Framework

For the purposes of this Policy, the terms and definitions given in NIST Cybersecurity Framework v1.1 2018 apply. The Cyber Security Framework covers 5 key areas:
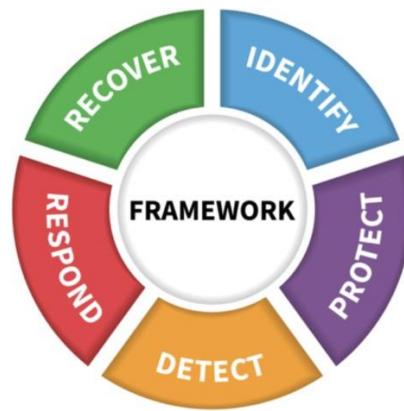
IDENTIFY

(ID.AM) Asset Management

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	Product 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 MEL internal and external systems. (e.g., AWS)		X	X

(ID.BE) Business Environment

MEL's Mission is *to change the way the world experiences property*. In doing so, we have an obligation (legally and ethically) to protect our customer, consumer, and confidential data.

Policy Objective	Accountable Role		
Accountable roles must:	All Staff	Product Staff	Technical Staff
Understand who they do business with and who can access handle and process MEL information, including:			
• Third parties • Technology providers • Suppliers and subsidiaries	X		
understand the regulatory frameworks that MEL must comply with, including:			
• Privacy • Financial services • Marketplace	X		

(ID.GV) Governance

As an ASX-listed organization, it is important that we manage our organization in a way that gives our shareholders confidence that we are managing risks within our macro-environment. In the case of cyber security risk – this includes the policies, procedures, and process that which drive our approach to managing cyber threats.

Policy Objective	Accountable Role		
Accountable roles must:	All Staff	Product Staff	Technical Staff
Escalate risks to the Executive Risk Committee (ERC) that may be outside MEL's risk appetite			
• Using appropriate group risk leads	X		

(ID.RA) Risk Assessment

Cybersecurity threats are one of many risks that could have a financial, reputational, legal, people or business continuity impact to MEL. 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	Product Staff	Technical Staff
Conduct a Security Impact Assessment when MEL information is being handled, stored or transmitted across networks or with third parties. Security impact 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	X
• Develop risk responses (treatments) and determine their prioritization		X	X

(ID.RM) Risk Management Strategy

MEL's Risk Management Framework (and its associated policies) is our guide for analyzing, mitigating and treating risk.

Policy Objective	Accountable Role		
Accountable roles must:	All Staff	ProductStaff	Technical Staff
Adhere to the MEL Risk Management Framework including:			
• Maintaining a risk register		X	X
• Reporting security risks that could be outside MEL's risk appetite	X		
• Implement or comply with security recommendations that are required to reduce, mitigate or manage a risk to an acceptable level	X		

(ID.SC) Supply Chain Risk Management

MEL's Procurement Policy is our guide for managing supplier and third-party risk.

Policy Objective	Accountable Role		
Accountable roles must:	All Staff	ProductStaff	TechnicalStaff
Manage cyber supply chain risk with suppliers and third-party partners, including:			
• Adherence to MEL's procurement policies, process, and procedures	X		
• Performing enhanced due diligence where criteria is met	X		
• Designing contracts that align to MEL's security risk appetite	X		
• Routine assessment of critical suppliers* to evaluate the are meeting their contractual obligations	X		
• routine assessment of response and recovery plans for critical suppliers*	X		

PROTECT

(PR.AC) Identity Management, Authentication & Access Control

Your MEL identity (just like your personal identity) is one of your most valuable assets.

If any MEL account is compromised, the identity can be used to gain the unauthorized access to valuable MEL 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	Product Staff	Technical Staff
Manage identities and credentials for systems where information is stored, used, or transmitted from, including:			
• Authorized devices and personnel		X	X
• Use unique identifiers		X	X
• Physical access		X	X
• Remote access		X	X
When building, changing, or maintaining access and authorization systems;			
• Authenticate users commensurate with the risk of the transaction (i.e. multi- factor for high-risk transactions or access to sensitive data)		X	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)			X
• ensure access remains assigned on a business-need-only basis[1]		X	X

1*Where access relates to a system or application in-scope for the Sarbanes-Oxley (SOX) program, user access management procedures (e.g., periodic reviews and timely offboarding) must be performed in accordance with requirements defined by the Risk & Assurance team.*

(PR.AT) Awareness & Training

The malicious 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 MEL identities. This helps us prepare for situations where the worst happens and what we can do to protect ourselves and MEL.

Policy Objective	Accountable Role		
Accountable roles must:	**All Staff**	**Product 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		

(PR.DS) Data Security

MEL 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 several security tools which provide the acceptable levels of control required for an ASX 100 organization, which is subjected to the Privacy Act.

Policy Objective	Accountable Role		
Accountable roles must:	**All Staff**	**Product Staff**	**Technical Staff**
Manage and protect MEL Data Assets;			
• Throughout their lifecycle (including creation, transfer, and destruction)	X		
• Supported by adequate capacity planning		X	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
• Protected against unauthorized 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		
• Segregated between development / test and production environments		X	X

(PR.IP) Information Protection Processes and Procedures

Security Policies (like this one) provide an overarching framework for MEL personnel to ensure we're managing our security responsibilities in line with our risk appetite for data loss.

Policy Objective	Accountable Role		
Accountable roles must:	All Staff	Product Staff	Technical Staff
Create, maintain, and implement policies, processes, and procedures in the following areas:			
• A baseline configuration of information technology they operate			X
• A system development life cycle		X	X
• Backups of information		X	X
• Data destruction		X	X
• Continuous improvement processes (e.g. PIRs, retros)	X		
• Vulnerability management		X	X
• Physical security of buildings and data centers			X
Report the effectiveness of protection technologies, including			
• Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) for high-priority systems		X	X
• Testing response and recovery plans at agreed intervals for high priority systems		X	X
• Cybersecurity in human resources practices (e.g., de-provisioning, personnel screening)		X	X

(PR.MA) Maintenance

When third parties manage assets on behalf of MEL, we are trusting them in our environment. Just like we trust a repairman in our own home, we need to ensure that if for any reason they go outside the scope of their engagement, we're aware and alerted to this activity.

Policy Objective	Accountable Role		
Accountable roles must:	All Staff	Product Staff	Technical Staff
ensure when maintenance and repair of organizational assets are performed by a third party:			
• Work is logged in a timely manner, with approved and controlled tools	X		
• Work is approved and performed in a manner that prevents unauthorized access, including adequate remote management protection (e.g., through the use of a VPN and short-lived credentials)		X	X

(PR.PT) Protective Technology

Just like a flight recorder in a plane, we need to ensure that if a system fails – we have accurate logging to ensure that we can identify the root cause and continuously improve our protection mechanisms. The same logic applies when we are referring to security protection mechanisms.

Policy Objective	Accountable Role		
Accountable roles must;	All Staff	Product Staff	Technical Staff
Design protective security technologies that ensure:			
• Communications and control networks(i.e., management networks) are protected		X	X
• Audit/log records are determined, documented, implemented, and reviewed		X	X
• Removable media is protected	X		
• Resilience requirements in normal and adverse situations are met		X	X

DETECT

(DE.AE) Anomalies and Events

We need alerting to ensure any activity that occurs outside the "norm" is identified and investigated by the appropriate party. If we don't identify these "spot fires" we may end up with a "wildfire" which is a lot harder to manage.

Policy Objective	Accountable Role		
Accountable roles must;	All Staff	Product Staff	Technical Staff
Build application and system detection processes and procedures for security events that includes:			
• A baseline of network operations and expected data flows for employees and systems			X
• The ability to analyze detected events to understand attack targets and methods			X
• Aggregate and correlate from multiple sources and sensors and establish incident alert thresholds			X
• Determining the impact of events		X	
• Establishing incident alert thresholds		X	

(DE.CM) Security Continuous Monitoring

The malicious people who target MEL 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	Product Staff	Technical Staff
Monitor the following for cybersecurity events:			
• The network			X
• The physical environment			X
• External service provider activity		X	X
• Unauthorized activity by personnel, devices and software			X
• Unauthorized mobile code			X
Vulnerability scans must be performed to:			
• Continually identify exposures			X
• Detect unauthorized mobile code			X

(DE.DP) Detection Processes

We need to make sure we define our detection processes within our squads, or better yet – at a tribe level. Consistent detection processes allow us to have greater confidence in our ability to detect potential security events. To ensure these processes are working as defined, regular testing is an imperative.

Policy Objective	Accountable Role		
Accountable roles must:	All Staff	Product Staff	Technical Staff
Build detection processes and procedures for security events, which:			
• Have well defined roles and responsibilities		X	X
• Are appropriately tested			X
• communicate event detection information to appropriate parties		X	X
• Are continuously improved			X

RESPOND

(RS.*) Response Planning, Analysis, Mitigation, Communications & Improvements

If the worst happens, it's important to have a plan. MEL 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 minimized and teams can get back to doing what they do best, quicker.

Policy Objective	Accountable Role		
Accountable roles must:	**All Staff**	**Product Staff**	**Technical Staff**
Execute response plans during or after an event, for which:			
• Personnel know their roles and order of • Operations when a response is needed	X		
• Events are reported consistent with established criteria	X		
• Information is shared consistent with response plans	X		
• Coordination with stakeholders is consistent with response plans	X		
• Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	X		
• Notifications from detection systems are investigated			X
• Vulnerabilities are disclosed to the organization by internal/external sources			X
• Manage incidents, ensuring:			
• The impact of the incident is understood	X		
• Incidents are categorized consistent with response plans		X	X
• They are contained		X	X
• They are mitigated		X	X
• Forensics are performed			X

RECOVERY

(RC.*) Recovery Planning, Communications & Improvements

Business Continuity Planning is for the worst-case scenario, for which incidents cannot be recovered within the allocated recovery time or data point.

Policy Objective	Accountable Role		
Accountable roles must:	**All Staff**	**Product Staff**	**Technical Staff**
Create, maintain and rehearse recovery to be executed during or after an event, which must include:			
• Lessons learnt incorporated into future recovery strategies	X		
• Management of public relations (external communication)		X	