

AEMO COMPLIANCE FRAMEWORK

PREPARED BY: Audit and Compliance team

DOCUMENT REF: RC-C01

VERSION: 1.0

EFFECTIVE DATE: April 2022

STATUS: Final

Approved for distribution and use by:

APPROVED BY: Tony Chappel, EGM Corporate Affairs, Legal, Risk & Governance

SUBMITTED BY: Audit and Compliance team

DATE: 02 May 2022

VERSION RELEASE HISTORY

Version	Date	Author	Peer Review	Approved	Changes	Next Review Date
0.1	5 Feb 2010	Evy Papadopoulos	Not specified	Board	Original Draft for Risk and Audit Committee	
0.2	22 Apr 2010	Louise Thomson	Not specified	Board	Draft updated to reflect Board comments: <ul style="list-style-type: none"> • Removed descriptive text in favour of a more streamlined document • Included explicit reference to identifying and testing key controls • Adopted more consistent language and terminology 	04/2012
0.3	7 Mar 2012	Mitchell Ajduk	Not specified	Board	Minor updates to reflect organisational and process changes and the revised breach impact matrix	03/2014
0.4	16 Jan 2019	Mitchell Ajduk	Brett Hausler	Board	Updated to incorporate: <ul style="list-style-type: none"> • Mandatory Data Breach Notification requirements under the <i>Privacy Act 1988</i> • Alignment with AS ISO19600:2015 Compliance Management Systems • Incorporation of WA compliance process • Process changes • Content refresh 	01/2021
1.0	02 May 2022	Rosalie Grant	Audit & Compliance team	EGM Corporate Affairs	<ul style="list-style-type: none"> • Reference to <i>Modern Day Slavery Act 2018</i> • Content refresh • Alignment with ISO37301:2021 Compliance Management Systems 	05/2024

CONTENTS

1.	INTRODUCTION	4
1.1.	Purpose	4
1.2.	Glossary	4
1.3.	Related AEMO Policies and Procedures	5
2.	COMPLIANCE POLICY	5
3.	ROLES AND RESPONSIBILITIES	5
3.1.	Roles and Responsibilities	6
3.2.	Resourcing	7
4.	COMPLIANCE MONITORING	7
4.1.	Compliance monitoring approach	8
4.2.	Identifying compliance obligations	9
4.3.	Input into monitoring method	9
4.4.	Monitoring and reporting	10
5.	MANDATORY DATA BREACH NOTIFICATION REGIME	11
5.1.	Personal Information	11
5.2.	What is a data breach?	11
5.3.	Responding to data breaches	11
6.	CONTINUOUS IMPROVEMENT	12
APPENDIX A.	IMPACT RATING MATRIX	13
APPENDIX B.	INTERNAL BREACH ESCALATION MATRIX	14

TABLES

Table 1	Abbreviations.....	4
Table 2	Defined terms	5
Table 3	Related policies, procedures, instructions, and forms	5

FIGURES

Figure 1	Compliance monitoring approach	Error! Bookmark not defined.
----------	--------------------------------------	-------------------------------------

1. INTRODUCTION

The Australian Energy Market Operator (AEMO) is a not-for-profit public company limited by guarantee, incorporated under the *Corporations Act 2011*. AEMO is the independent electricity and natural gas system planner and system and market operator for the National Electricity Market (NEM), the Victorian Declared Shared Network (DSN), the Victorian Gas Declared Transmission System (DTS), the Declared Wholesale Gas Market (DWGM), Short Term Trading Markets (STTM), the Gas Supply Hub (GSH), Gas Bulletin Boards (GBB) and the Western Australian Wholesale Electricity Market (WEM).

As the independent system and market operator, AEMO's primary responsibility is the design and operation of a sustainable energy system that provides affordable, safe, and reliable energy for all Australians. To help maintain energy system security it is important that AEMO is diligent in fulfilling its obligations.

AEMO is subject to numerous compliance obligations under Federal and State legislation and energy industry specific legislation. By implementing an effective compliance framework, AEMO will be positioned to meet, and to demonstrate that it meets, its compliance obligations. Further, by understanding and managing compliance risk, AEMO can make better informed decisions and provide greater certainty and confidence to our stakeholders, employees, and the markets in which we operate.

1.1. Purpose

The purpose of this document is to:

- (a) Articulate AEMO's approach to compliance management, developed in accordance with ISO 37301:2021
- (b) Describe the roles and responsibilities for compliance that different parts of the organisation are required to discharge
- (c) Define the process AEMO has in place to identify, respond and report alleged breaches of our compliance obligations
- (d) Describe how AEMO updates obligations resulting from rule changes

1.2. Glossary

Table 1 Abbreviations

Abbreviation	Meaning
AEMO	Australian Electricity Market Operator
AEMC	Australian Energy Market Commission
AER	Australian Energy Regulator
ERA	Economic Regulation Authority
NEL	National Electricity Law
NER	National Electricity Rules
NEM	National Electricity Market
WEM	Wholesale Electricity Market (WA)
NGR	National Gas Rules
GSI	Gas Services Information (Rules)

Table 2 *Defined terms*

Term	Definition
Regulatory obligations	A need or expectation that is stated, generally or obligatory, that AEMO must comply with
Compliance risk	The risk of legal or regulatory sanction, financial or reputational loss arising from our failure to abide by the compliance obligations required of AEMO.
Regulatory obligations	The requirements set out in legislation, regulation, licence conditions to which AEMO subscribes. Obligations arising out of contractual arrangements with AEMO are excluded from this definition.

1.3. Related AEMO Policies and Procedures

This Framework is aligned with and should be read in conjunction with other internal policies, procedures, and guidelines, of which several are listed below.

Table 3 *Related policies, procedures, and guidelines*

Title	Title
AEMO Risk Management Framework	Document Retention Policy
AEMO Risk Management Policy	Fraud and Corruption Prevention Policy
Code of Conduct	Grievance Resolution Policy and Guidelines
Breach Management Procedure	Introduction to Compliance at AEMO
Compliance Policy	Responding to Data Breaches
Confidentiality Guidelines	Whistleblower Protection Policy
Confidential Information Policy	Whistleblower Protection Procedures
Discipline Policy and Procedure	WHSE Policy

2. COMPLIANCE POLICY

Underpinning the Compliance Framework is the Compliance Policy (Policy). The Policy provides a statement of AEMO's commitment to maintain compliance with all relevant laws, rules and regulations (referred to as 'regulatory obligations'). It provides high level details on AEMO's compliance commitments and roles and responsibilities for compliance. A copy of the Policy is located on MO.

3. ROLES AND RESPONSIBILITIES

While the effective identification and management of compliance with regulatory obligations is the responsibility of every employee at AEMO, there are several specific responsibilities allocated to various parts of the organisation. The following sections set out the people who have a role or function under the Compliance Framework (specified by position or group as appropriate), and briefly describes their responsibility.

3.1. Roles and Responsibilities

Role	Responsibility
The Board	<ul style="list-style-type: none"> • Providing oversight of compliance with ethical, legislative, and regulatory requirements • Ensuring a compliance system is implemented, updated regularly, setting out AEMO's major legal obligations and its compliance with those obligations
Risk and Audit Committee	<ul style="list-style-type: none"> • Monitoring the development and ongoing review of appropriate legislative and regulatory compliance programs (excluding work, health, safety, and environment) • Reviewing any instances of breaches or non-compliances • Reviewing compliance with exemption criteria and reporting requirements (e.g., Australian Financial Services Licence) • Monitoring corporate governance policies and procedures to ensure they are appropriate and reviewed on a regular basis
Chief Executive Officer (CEO)	<ul style="list-style-type: none"> • Establishing and maintaining effective processes for managing compliance throughout AEMO • Demonstrating commitment to designing, implementing, maintaining, and improving an effective compliance framework • Leading by example in the establishment of a culture of transparency and compliance awareness • Clearly communicating with all stakeholders and employees the standard of compliance adopted by AEMO • Ensuring policies, procedures and processes that support the achievement of AEMO's obligations are in place • Allocating adequate resources for compliance activities
Executive General Managers (AEMO's Executive Leadership Team)	<ul style="list-style-type: none"> • Supporting the CEO in establishing and maintaining effective processes for managing compliance throughout AEMO • Leading by example in the establishment of a culture of transparency and compliance awareness. • Ongoing communications that support the importance of an effective compliance management system • Ensuring effective and timely compliance reporting • Agreeing to be measured against key compliance performance measures and outcomes
Group Managers	<ul style="list-style-type: none"> • Developing, implementing, maintaining and ongoing review of appropriate processes and procedures for the identification, monitoring and reporting of all obligations within their area of responsibility. • Actively participating in the management and resolution of compliance incidents and issues, including potential or actual breaches • Actively encouraging, mentoring, coaching and supervising employees to promote compliant behaviours and encourage employees to raise compliance issues and incidents • Developing employee awareness of regulatory obligations and requiring them to meet training and competence requirements

Role	Responsibility
Employees	<ul style="list-style-type: none"> • Being aware of and adhering to the regulatory obligations relevant to their roles • Being aware of and adhering to policies and procedures relevant to their roles • Monitoring performance and testing of their controls to maintain compliance • Reporting any identified actual or potential noncompliance in a timely manner • Undertaking any necessary training • Contributing to the continuous improvement of the Compliance Framework
Audit and Compliance team	<ul style="list-style-type: none"> • Ensuring obligations are current and maintained within the obligation register • Providing support to management and employees in the pursuit of compliance management responsibilities • Coordinating compliance management reporting and ensuring consistency of approach including breach reporting • Liaising with regulators • Researching and providing staff with compliance management tools and methodologies • Organising appropriate staff training • Demonstrating, through a program of audit and review those systems used to identify and achieve compliance outcomes remain effective and compliant
Internal and External Auditors (incl. Market Auditors)	<ul style="list-style-type: none"> • Providing assurance to the Board and Board Committees on the adequacy and effectiveness of our compliance program and control environment

3.2. Resourcing

The core elements of the Compliance Framework are integral to normal business operations. Specific provision is made in the AEMO budget for the allocation of resources that support compliance management. Where appropriate to do so, working groups may be used to fully understand compliance obligations and the implications for AEMO.

4. COMPLIANCE MONITORING

An essential element of the Compliance Framework is the identification, assessment and monitoring of compliance with obligations. Our compliance monitoring process has been aligned to ISO 37301:2021, that defines how we identify, respond and report compliance matters, including alleged breaches.

AEMO has a range of obligations across a variety of laws, rules, and regulations. This incorporates non-energy and energy market obligations. It is important for the integrity of the markets that AEMO operates, that AEMO complies with, and can demonstrate its compliance with, these obligations. The process flow displayed in Figure 1 below shows the key steps of AEMO's compliance monitoring approach:

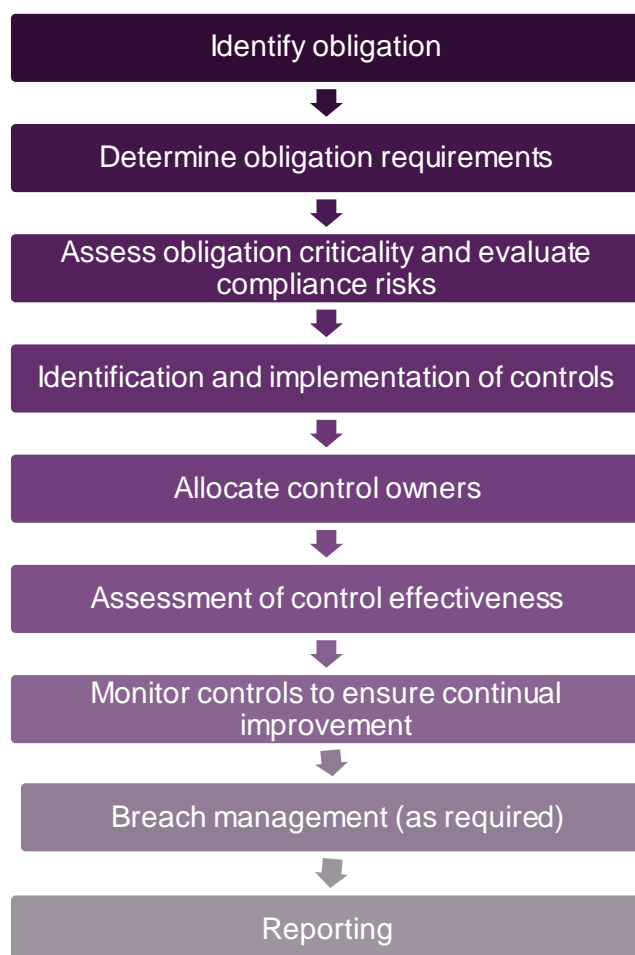


Figure 1 Compliance monitoring approach

4.1. Compliance monitoring approach

AEMO's obligations are identified and recorded in an obligation register. If any breach occur, they are lodged and reported. The approach to monitoring compliance with regulatory obligations is aligned with AEMO's risk-based approach to decision-making. This allows resources to be focused on areas where there are greater risks to AEMO from a regulatory, reputation, liability, safety, infrastructure, or financial perspective.

The multi-tiered approach applied covers:

- a) Obligations that are assessed as having an *extreme, major, or moderate* impact in the event of a breach will be incorporated into a compliance monitoring system that will actively monitor AEMO's ongoing compliance with obligations.
- b) Obligations that are assessed as having an *immaterial or minor* impact in the event of a breach may not be included in the regular monitoring. Any such obligations will be reported only in the event of a breach, using the breach reporting process.
- c) Spot checks or self-assurance activities may be undertaken to provide assurance that compliance with targeted obligations is being maintained. These activities may focus on obligations not included in the routine monitoring.
- d) Some requirements, such as obligations relating to protected information, may not be suited to a compliance monitoring approach. This is because the instances in which these obligations are

activated are too numerous or they apply to too many people. In such cases, a communication campaign, in which general communications are issued to staff reminding them of their compliance obligations and the requirement to report any breaches, is more effective.

The decision regarding which review method is applied to an obligation will be made by the Audit and Compliance team in consultation with the process owners and Legal team where necessary, based on the data that has been collected.

4.2. Identifying compliance obligations

AEMO operates in a highly regulated industry and has a significant number of compliance obligations at both the Commonwealth and State level. To ensure AEMO complies with all its obligations, it is important to identify legislation and other legislative instrument which impose a compliance obligation. This section describes the process for identifying changes to laws, rules and regulations that have an impact on AEMO.

4.2.1. Changes to laws, legislation, and regulations

The expertise required to identify and assess proposed changes to the various laws, rules and regulations that impact on AEMO is not concentrated in a single area.

The Audit and Compliance team monitors a range of websites and has established subscriptions to receive updates and changes in laws, legislation, and regulations. Rule changes are centrally captured and implemented through engagement with representatives from departments across AEMO.

External Affairs (Market Regulation) is responsible for tracking and managing any Rule change through a process involving relevant stakeholders across AEMO and regular liaison with the Audit and Compliance team.

Once a final determination has been announced, the Audit and Compliance team liaise with representatives from the business departments to ensure any change is understood and appropriate controls implemented.

In the event, a new piece of legislation is enacted (example: *Modern Slavery Act 2018*), a working group may be formed to fully understand the obligations imposed on AEMO and ensure mitigating controls are in place and where necessary, monitored for improvement.

4.2.2. Assessment of Criticality of Compliance Obligations

Achieving an accurate and informed rating for each obligation requires input from individuals with operational expertise and responsibility for compliant outcomes.

AEMO has developed a matrix that facilitates the assessment of its risk of noncompliance, using a combination of likelihood and the consequence. Using this approach to assessing obligations enables suitable effort to be expended on those obligations that represent the greatest threat to AEMO or the operation of the market and systems. This assessment is based on the impact (consequence) of an obligation breach (refer to Appendix A for more detail) and inform the type of controls and monitoring required.

4.3. Input into monitoring method

Management is responsible for nominating obligation owners and ensuring adequate controls are in place to mitigate noncompliance risk and prevent noncompliance arising. Controls are required to be input into the obligation register for ongoing monitoring via assurance activities or exception reporting.

4.4. Monitoring and reporting

4.4.1. Review of compliance obligations

In addition to regular surveys, spot checks and breach reporting, which are typically geared towards self-assessment of controls, the Audit and Compliance teamwork with Internal and Market Auditors to identify key controls (such as operating procedures or automated systems) to be tested in each audit cycle.

4.4.2. Whistleblower protection

AEMO actively encourages the raising of concerns, and the Whistleblower Protection Policy prohibits any form of retaliation for doing so.

4.4.3. Internal reporting of alleged breaches

A breach is an act or omission leading to AEMO failing to meet its compliance obligations. A compliance breach can be unintentional or deliberate. Deliberate or negligent breaches of AEMO's compliance obligations are not tolerated. All potential or actual compliance breaches must be reported to the Audit and Compliance team, in consultation with the employees' Manager, and as required, the Legal team.

All potential or actual compliance breaches must be reported using the Compliance Breach Form, located on MO, and submitted to the Audit and Compliance team, and assessed in accordance with the Breach Impact Matrix detailed in Appendix A.

AEMO's internal breach reporting process is:

1. *Identification* – A potential or actual breach is identified and reported to the Audit and Compliance team via a completed Compliance Breach form
2. *Assessment* – The potential or actual breach is investigated by the relevant business team, with assistance from the Audit and Compliance team and legal to determine immediate corrective actions, consequences, and longer-term remediation plans to rectify the breach and mitigate reoccurrence
3. *Escalation* – Once an actual breach is determined, depending on the severity and nature, it may be escalated internally, in accordance with the Breach Escalation Matrix specified in Appendix B,
4. *Reporting*: The results of compliance monitoring, and analysis of any trends or issues identified through monitoring are reported quarterly to the RAC

4.4.4. External breach reporting

Economic Regulation Authority (ERA)

Legislation requires AEMO to support the ERA, Western Australia's regulatory body, with its compliance functions. All instances of alleged breach of the Wholesale Electricity Market Rules and Gas Services Information Rules by AEMO and Market Participants must be reported. To meet this obligation, AEMO provides periodic alleged breach reports to the ERA.

The ERA make the final determination on whether a breach has occurred, including instances where AEMO has self-reported an alleged breach to the ERA.

The Market Procedure and the Monitoring and Reporting Protocol details the relationship between AEMO, and the ERA and its compliance reporting processes.

Australian Energy Regulator (AER)

AEMO reports to the AER as required and requested basis unless otherwise specified within legislation. Where mandatory reporting of a compliance breach is required, the Legal team will be consulted prior to submission to the AER.

Consequences of non-compliance

Penalties for non-compliance can include fines, increased regulatory oversight and external reporting requirements, increased regulation, enforceable undertakings, stop work orders and suspension or withdrawal of operating licences. In some instances, non-compliance could result in individual penalties, as well as penalties for AEMO. Non-compliance can also damage AEMO's reputation with external stakeholders.

5. MANDATORY DATA BREACH NOTIFICATION REGIME

This section sets out the process that AEMO staff should follow if AEMO experiences a data breach or suspects that a data breach has occurred.

5.1. Personal Information

AEMO is committed to protecting the privacy of personal information. AEMO collects, holds, and discloses (where required) personal information in its capacity as the major market and system operator of energy markets in Australia. 'Personal information' includes any information or opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who may be reasonably identified. This includes (but is not limited to) the information that AEMO holds in relation to participants in the gas and electricity markets, government departments, industry associations, consumers, contractors, and employees.

AEMO is subject to the *Privacy Act 1988 (Cth)* (Privacy Act), which regulates the way personal information is handled. Under the requirements in the Privacy Act, AEMO must notify the Office of the Australian Information Commissioner and affected individuals as soon as practicable in the event of an 'eligible data breach' of personal information. AEMO must conduct and complete an assessment of a suspected data breach within 30 days after becoming aware that there are reasonable grounds to suspect that the breach has occurred.

5.2. What is a data breach?

A 'data breach' occurs when confidential information is lost in error, or becomes vulnerable to unauthorised access, modification, use or disclosure, or other misuse or interference.

Data breaches are not limited to malicious actions like theft or 'hacking'. It can include human error and mishandling resulting in accidental loss or disclosure. This can happen if an email is sent to the wrong address or a device containing data is lost or stolen. Releasing information to unintended third parties can cause harm to the individuals and businesses impacted.

A data breach is an 'eligible data breach' where a reasonable person would conclude there is a likely risk of 'serious harm' to the affected party because of unauthorised access or unauthorised disclosure of confidential information. 'Serious harm' may include reputational damage, physical, emotional, economic, and financial harm.

5.3. Responding to data breaches

Data breaches must be dealt with on a case-by-case basis by undertaking an assessment of the risks involved and using the risk assessment to decide the appropriate course of action. For the process for responding to data breaches, refer to the *Responding to Data Breaches*.

The following documents are available on MO to assist with responding to a potential data breach:

- Data Breach Incident Form; and
- Data Breach Investigation Form.

6. CONTINUOUS IMPROVEMENT

The Audit and Compliance team is responsible for improving the overall effectiveness of the Compliance Framework, and to embed compliance management into operational policies, processes and procedures, independent from business operations. Regular monitoring and review of the Compliance Framework and related policies and procedures provide a continuous feedback mechanism between the ELT, the RAC and the Board.

The Audit and Compliance team are available to provide advice and support to staff in the management of obligations, controls, and mitigations to reduce the risk of noncompliant outcomes.

APPENDIX A. IMPACT RATING MATRIX

AEMO Breach Impact Matrix

Type of Impact	EXTREME	MAJOR	MODERATE	MINOR	IMMATERIAL
Reputation & Stakeholders	Significant long-term damage to stakeholder confidence and relationships Continued adverse media exposure Significant financial impact drives participant(s) towards insolvency	Significant short term damage to stakeholder confidence and relationships Short term adverse media exposure Significant financial impact on participant(s)	Some damage to stakeholder confidence and relationships Some adverse media exposure Adverse financial impact on participant(s)	Manageable reduction in stakeholder confidence Limited media exposure Limited to no financial impact on participant(s)	No lasting reduction in stakeholder confidence No media exposure No financial impact on participant(s)
AEMO Financial Impact	>\$25M	>\$5M-25M	>\$500K-\$5M	>\$100K-\$500K	<\$100K
People* (Health & Safety, Workforce)	Single fatality, severe permanent injury or multiple notifiable injuries, or life threatening exposure to a health risk Workforce impact across AEMO causing an inability to deliver core functions and/or strategy implementation over a sustained period	Injury or illness requiring > 5 days hospitalisation or medical treatment (incapacity beyond 3 months) Workforce impact causing an inability to deliver some core functions and/or strategy implementation	Injury or illness requiring < 5 days hospitalisation or medical treatment and/or counselling services or intervention (6 days to 3 months incapacity) Workforce impact in multiple areas but not impacting delivery of core functions and/or strategy implementation	First aid or counselling services required (not sustained) due to an incident which does not restrict employees from performing their roles Workforce impact within one department but no impact to delivery of core functions and/or strategy implementation	Near miss, no medical or first aid treatment required Workforce impact limited to local team but not impacting delivery of core functions and/or strategy implementation
Environment	Permanent long term environmental harm, e.g. major pollution incident causing significant damage or potential to health or the environment Fines and prosecution likely	Long term or serious environmental damage (extensive rectification activity required) Multiple complaints received Potential for prosecution	Measurable environmental impact (significant rectification required) Will cause complaints Possible fine	Measurable environmental harm (no or minimal rectification required) Potential for complaints Fine unlikely	No environmental harm No fines or complaints
Market & System	Loss of supply to a state(s) for any duration (e.g. system black) Market suspension market(s) for a prolonged period	Loss of supply to a large portion* of a state, for any duration Market suspension in one jurisdiction or market for a short period	Localised/minimal loss of supply in a state Market(s) in administered state or material scheduling error	Intervention required to maintain supply Immaterial scheduling error (below dispute threshold)	No restriction of supply No disruption to markets
Legal & Regulatory	Corporate fine >\$1M Imprisonment and/or disqualification to Officer or Director Government inquiry on AEMO's functions Litigation involving Class actions	Corporate fine or civil penalty \$100K to \$1M and/or court enforceable undertaking Fine for personal liability to Officer or Director Sustained Regulator scrutiny requiring extensive management effort to address Litigation involving protracted Court actions possible	Fine of less than \$100K and no personal liability Regulator or government inquiry with loss of reputation or adverse government impact	Nominal fine Regulator or government inquiry resolved by routine management procedures	No fine No government or regulator inquiry

APPENDIX B. INTERNAL BREACH ESCALATION MATRIX

Breach Rating	Chief Executive Officer	Executive General Manager	Group Manager	Audit and Compliance	Purpose of Communication
Extreme	Immediately	Immediately	Immediately	Immediately	<ul style="list-style-type: none"> • Immediate action needed at all management levels to address the issue. • The CEO advised for information purposes (and potentially decision-making purposes). • CEO will determine whether escalation occurs to AEMO Board.
Major	Within 24 hours	Immediately	Immediately	Immediately	<ul style="list-style-type: none"> • Immediate action needed at Executive Management levels to address the issue. • The CEO advised for information purposes and CEO will determine whether escalation occurs to AEMO Board.
Moderate	No notification required	Within 24 hours	Immediately	Immediately	<ul style="list-style-type: none"> • Immediate action needed at all management levels to address the issue. • Advice to Executive Manager responsible.
Minor	No notification required	Within 48 hours	Within 24 hours	Within 24 hours	<ul style="list-style-type: none"> • Action needed at General Manager levels to address the issue. • Advice to Executive Manager responsible for information purposes.
Immaterial	No notification required	Within 72 hours	Within 24 hours	Within 24 hours	<ul style="list-style-type: none"> • Action needed at General Manager levels to address the breach. • Advice to Executive Manager responsible for information purposes.