




Adani Wilmar Limited
IT Security & Data Privacy Policy

1. Introduction & Objectives

IT security policy is focused on protecting the security of Adani Wilmar information and assets. Adani Wilmar is also committed to establishing and improving cyber security preparedness and minimizing its exposure to associated risks to safeguard assets. All AWL businesses and functions will implement adequate security policies, processes, and controls to protect confidentiality, maintain integrity, and ensure availability of all information assets.

The objective of IT & cyber security policy is to:

- a) Establish a robust framework that safeguards the confidentiality, integrity, and availability of its information assets.
- b) Prevent unauthorized access, modification, or disclosure of sensitive information, ensuring its accuracy and reliability.
- c) Maintain the availability of information and mitigate risks by identifying, assessing, and addressing potential threats.
- d) Implement control and monitor measures for all hardware and software assets in use throughout the organization
- e) Compliance with relevant & applicable national & international laws and standards
- f) Identify risks to information and cyber systems and mitigate to acceptable level through a formal documented procedure.
- g) Protect critical information from unauthorized access, use, disclosure, modification and disposal, whether intentional or unintentional.
- h) Conduct regular cyber-security audits following appropriate national and international standards to maintain compliance.
- i) Communicate the importance and ensure that all concerned stakeholders understand their responsibilities and roles regarding IT & cyber security.
- j) All Business Heads/Department Heads are directly responsible for ensuring compliance with this policy in their respective business domains.
- k) All breaches of information security, actual or suspected, are reported, investigated by the designated personnel and appropriate corrective and preventive actions initiated.
- l) Establish clear-cut reporting channels for any form of violation of the Cyber Security and Data Privacy policies and any other specific information security and management policy as the case may be.
- m) Protect AWL stakeholders, information and assets from threats that could potentially disrupt business and Adani Wilmar brand and reputation.
- n) Reduce the risks due to human error, theft, fraud, or misuse of IT assets.
- o) Reduce the number of adverse incidents.

	<p style="text-align: center;">Adani Wilmar Limited IT Security & Data Privacy Policy</p>
---	---

- p) Restrict access to the information assets as per the business requirement.

2. Scope & Applicability

This policy applies to all employees, subsidiaries, contractors, partners, and interns working in the company. Third party service providers providing services to the company or wherein data is held outside premises, shall also comply with this policy. Scope of this IT policy is the information stored, communicated, and processed within the company and the company's data across outsourced locations.

This policy applies to all stakeholders who access AWL's information or networks: Full Time Employees (FTE), Off-roll employees, including but not limited to subsidiary staff, contractors, consultants, temporary staff affiliated with third parties, including system vendors and staff from outsourcing companies. This policy also applies to all information, computer and data communication systems owned, licensed, and administered by AWL or its service providers and covers manifestations of other AWL's information such as voice and data.

The content and robustness of implementation of this policy will be reviewed periodically and revised accordingly, as needed.

3. IT Security Roles and Responsibilities


The company has formed an information security management committee, which consists of the ISC (Information Security Committee) and Information Security operations team who will implement and manage information security in the organization.

4. Policy Management and Compliance

- a) IT Security Policy shall be accessible to all employees of the company. All employees should read the policy, understand their responsibilities, confirm acceptance and should ensure information security
- b) The policy shall be reviewed once a year and/or as & when required
- c) The policy shall be reviewed and approved by ISC. All changes to policy shall be communicated by the ISC and/or, CISO to all employees and third-party personnel through appropriate forums and channels.

Compliance

- a) All employees, stakeholders and third-party vendors, contractors, interns, trainees, and consultants shall comply with IT policy.

	Adani Wilmar Limited IT Security & Data Privacy Policy
---	---

- b) Any violation or any attempted violation of the IT security policy shall result in disciplinary action taken in consultation with ISC.

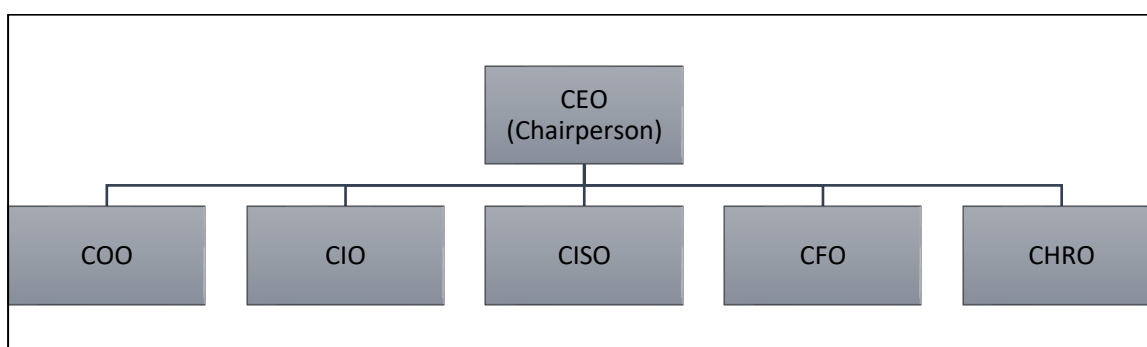
5. Organization of IT Security Committee


The members who participate in the Information Security Committee are critical to the success of the company's information security program. The Information Security Committee is a cross-functional group comprised of employees representing different parts of the organization.

The following table lists the members of the IT Security Committee:

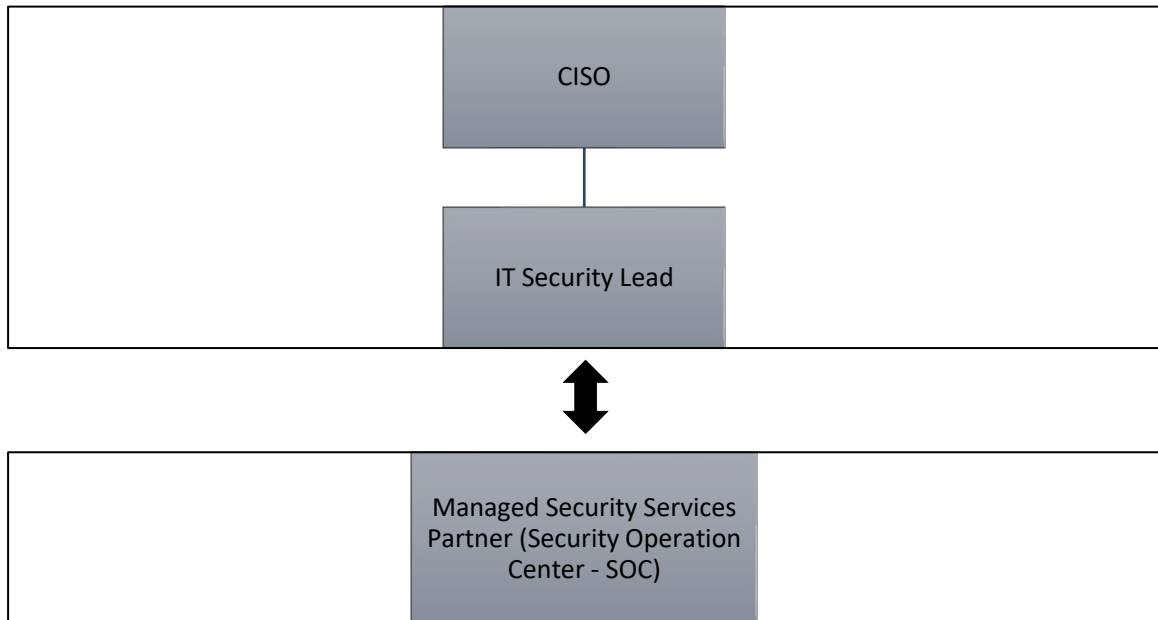
Member Designation	Role
CEO and MD	Chairperson
CIO (Chief Information Officer)	Member
CHRO (Chief Human Resources Officer)	Member
CFO (Chief Financial Officer)	Member
COO (Chief Operations Officer)	Member
CISO (Chief Information Security Officer)	Member

Organization Chart:



	<p align="center">Adani Wilmar Limited IT Security & Data Privacy Policy</p>
---	--

IT Security Operations team




6. Asset Management

- a) All company IT assets shall be procured as per company-wide asset procurement process.
- b) The asset owner shall be responsible for the appropriate classification, maintenance, and protection of information.
- c) The company IT must ensure that all employees and external party users should return company assets on termination/exit of their employment.
- d) An appropriate set of procedures for IT Asset labelling should be developed and implemented with the information classification scheme.
- e) The IT Security Operations team is responsible for user access management, password management, and role management.

7. Incident Management

- a) Management responsibilities and procedures should be established to ensure a quick and effective incident management.
- b) Information security events in the company should be reported through appropriate management channels as quickly as possible.
- c) Information security incidents should be responded according to the documented procedures.

	<p style="text-align: center;">Adani Wilmar Limited IT Security & Data Privacy Policy</p>
---	---

- d) Records shall be maintained for all security incidents and stored in a manner to prevent unauthorized access or modification.

8. Business Continuity Management

- a) The company should determine its requirements for continuity of IT security management in adverse situations.
- b) The company should verify established information security controls at regular intervals to ensure they are valid and effective during adverse situations.
- c) Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.

9. Data & Cloud Security

- a) All the files store in the shared folders of the local share drives/servers shall be classified accordingly. All company devices will have full disk encryption enabled for securing company data.
- b) Master Service Agreements (MSA) and Non-Disclosure Agreements (NDA) with cloud service providers shall be reviewed, understood, and accepted before sign-up to the service and accept.
- c) Contracts involving personal data shall be checked to ensure that they comply with applicable data protection legislation. If not, a separate data processing agreement may be required.
- d) As per the statutory requirement, audit logging shall be available to understand the ways in which data is being accessed and to identify whether any unauthorized access has occurred.

10. IT Supplier Management

- a) All third parties are required to sign and submit specified documents such as the Master Service Agreement (MSA), Non-Disclosure Agreement (NDA) etc. pertaining to information security prior to any engagement as per the company's third-party requirements.
- b) Legal and regulatory requirements, including data protection, intellectual property rights, copyrights should be met by the supplier.
- c) Awareness training for the third-party/supplier personnel shall be conducted to ensure that the information is handled securely.