Dairy Australia

INFORMATION TECHNOLOGY SECURITY POLICY

This policy outlines the minimum requirements for the protection of Dairy Australia's confidential information.

For internal Dairy Australia use and distribution only.

Once printed, this is an uncontrolled document.

Approved August 2022

Document Control

Version #	Reviewed By	Date	Endorsed By	Date	Approved By	Date	Summary of Change
01	GM BOP	August 2020	ARMC	August 2020	Board	September 2020	New policy which combines the following documents: • Antivirus Policy • Wireless Access Policy • Remote Access Policy • Password Policy
02	GM BOP	July 2022	ARMC	August 2022	Board	August 2022	Reviewed – minor updates and clarification of HR responsibilities

Document Steward	**IT Manager**
Document Owner	**General Manager, BOP**

Related Documents
IT Security Procedure
IT Acceptable Use Policy
IT Acceptable Use Procedure
Code of Conduct

Review Requirements
This document is next due for review in August 2024 by the General Manager BOP

Controlled Document Location
https://dairyaustralia.sharepoint.com/SitePages/documenthub.aspx

Contents

INFORMATION TECHNOLOGY SECURITY POLICY

1 Purpose

The purpose of this policy is to articulate Dairy Australia's information security requirements that ensure that Dairy Australia's confidential information and technologies are not compromised, and interests of Dairy Australia are protected.

2 Scope

This policy applies to all Dairy Australia employees   including fixed term, casual, Dairy Australia directors, contractors and all parties who access Dairy Australia's information technology infrastructure, hereinafter referred to as users. It also applies to all electronic information, data, software, hardware and communications networks owned or operated by, or on behalf of Dairy Australia.

This policy must be read in conjunction with the *Information Technology Security Procedure*, the *IT Acceptable Usage Policy* and the *IT Acceptable Usage Procedure.*

3 Policy Statement

Dairy Australia is committed to ensuring an appropriate level of security is applied to protect the confidentiality, integrity and availability of its information.

4 Policy Principles

- all users of information assets are responsible for information security
- external providers engaged by Dairy Australia must comply with this policy and associated procedures
- access to Dairy Australia's information is available only to those with a legitimate need
- information technology systems and solutions are designed, sourced, implemented, and operated in ways that are secure, sustainable, cost effective and aligned to Dairy Australia's strategy
- all users must ensure that passwords adhere to and are managed in accordance with the account security guidelines in the IT Security Policy Procedure document

5 Roles and Responsibilities

The table below documents the responsibilities of all roles involved in the security of Dairy Australia's information assets.

Role	Responsibilities
Dairy Australia Board	Ultimately responsible for ensuring that the organisation maintains information security, maintains sufficient IT security capability commensurate with risks and implements IT security controls to manage risks within the risk appetite
Dairy Australia information technology users	• Take responsibility for developing an adequate level of information security awareness to ensure appropriate use of the information environment • Only access information needed to perform their authorised duties • Must protect the confidentiality, integrity and availability of Dairy Australia's information and information stored by Dairy Australia • Must not in any way divulge, copy, release, sell, loan, alter or destroy any sensitive information without approval from the relevant General Manager • Must safeguard any physical key, ID card, computer/network account, or device provided by Dairy Australia that enables access to Dairy Australia's information. This includes maintaining appropriate account and password protection measures as set out in the IT Security Policy and Procedure documents. • Report any activities considered likely to breach this Policy or compromise sensitive information to the relevant Manager, General Manager or to the IT Manager • Protect sensitive information even after leaving Dairy Australia
IT Manager	• Implement appropriate information security controls and processes to protect DA from cyber security threats and detect any potential cyber security incidents • Implement secure user access management for all Dairy Australia authorised users • Educate users on how to reduce the risks of cyber security incidents • Undertake risk-assessments of the technology control environment and advise on information security risks and controls
Managing Director / General Managers / Regional Managers	• Ensure the IT Security Policy and Procedure are implemented within area of control • Ensure appropriate action is taken when the IT Security Policy and Procedure are breached

Role	Responsibilities
Contract Owners	Any agreement where a third party requires the following access must include references to the third party adhering to the Dairy Australia IT Acceptable Use Policy, IT Acceptable Use Procedure, IT Security policy, and IT Security Procedure: • creation of accounts (user or administrative), or use of Service Accounts that are hosted within a system managed by Dairy Australia • access to the Dairy Australia IT network (wired, wireless, remote access or any other means of access) • access to any Dairy Australia systems (cloud, hosted or otherwise) for the purposes of performing administrative, configuration or development work • access to documents shared by Dairy Australia using approved sharing methods is not applicable – refer to the IT Acceptable Usage Policy and Procedure for information on approved sharing methods • Reviewed – minor updates and clarification of HR responsibilities The Agreement should state that any third-party supplier not complying with these policies could have actions taken against them including but not limited to termination of contract.
Human Resources	• Provide training to all employees and contractors to raise awareness and understanding of the IT Security Policy and Procedures • Ensure all employees and contractors review and acknowledge the IT Security policy and procedure and undertake the IT security training online module on an annual basis • Provide reports to the GM BOP on training completion rates

6 Compliance and Assurance

- The GM BOP must ensure appropriate monitoring compliance processes are in place for this Policy
- Breaches of this Policy should be recorded as an incident

7 Review

In line with Dairy Australia’s Policy Governance Policy, this policy is scheduled for review every two years or more frequently if appropriate.