Dairy Australia

INFORMATION TECHNOLOGY SECURITY PROCEDURE

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 Procedure which combines the previous documents: • Antivirus Policy • Wireless Access Policy • Remote Access Policy • Password Policy
02	GM BOP	July 2022	ARMC	August 2022	Board	August 2022	Extend the policy to cover systems for external use Various updates to clarify account standards and types Addition of Access Management, SSO, SSPR and access from mobile devices Clarification of network security controls Clarification of ways security incidents can be generated Clarification that the policy applies to procurement or development of any IT system Addition of MFA as a compliance obligation Clarification of HR responsibilities
Document Steward							**IT Manager**
Document Owner							**General Manager BOP**

Related Documents
IT Security Policy
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 PROCEDURE

1 Purpose

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

2 Scope

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

IT will maintain an inventory of users, systems, applications, databases and platforms, together with system architecture, network architecture and data flows to document the scope of the IT environment.

3 Account Security

The section below describes the standards and measures in place relating to accounts used to access Dairy Australia's IT systems.

This applies to all IT systems including those developed/implemented for external access and use.

3.1 User access

User accounts are categorised into the following types:

- Normal user account
    - provided to full and part-time Dairy Australia staff and must be requested and approved via the HR onboarding process
- Guest user accounts
    - used for Accounts for consultants, contractors, casual staff or any other non-Dairy Australia users require IT Manager approval and require an expiry date to be set. Once the new HRIS system is implemented must be requested and approved via the HR onboarding process
- Administrative account

        - Accounts with privileged access, e.g. administrative accounts, must be approved by the IT Manager before they are created
- Generic account
    - will not be created for any purpose without IT Manager approval
- Service account
    - must not be created without IT Manager approval
    - must be created for each discrete purpose and are not to be shared between systems

3.2 Privileged account management

- Separation of administrative privileges is implemented on all core IT systems and elevated access is only provided to individual staff administrative accounts
- Administrative accounts are not to be used for day to day activities
- Scripting, automation, or any attempt to bypass the use of administrative credentials is not permitted
- Administrative access to any IT systems must be approved by the IT Manager or an approved delegate (e.g. technical owner of the application). This approval requirement cannot be delegated for core IT systems including Office 365, Active Directory, IT Password Vault, or any system where sensitive data is stored.

3.3 Password management

The following controls apply to all account types

- All account passwords (e.g. user or administrative accounts) must have password expiry enabled and passwords will be required to be changed at a maximum every 90 days
- All account passwords must have minimum length of eight characters
- The last four passwords cannot be used (password history)
- The IT Service Desk will reset user account or administration account passwords if a user cannot use their password for whatever reason. This password will be for a single use and must be changed at next login
- Accounts will be automatically locked after six incorrect attempts within a 15-minute period and can only be unlocked by IT, or the user by performing a self-service password reset.
- All accounts must have a unique password and passwords must not be reused between accounts
- No Dairy Australia passwords other than the passwords assigned to an individual are to be stored in local password managers or saved in the browser. Under no circumstances are generic, service account, master, or ‘break glass’ account details to be stored anywhere other than the Dairy Australia IT password vault
- All Service accounts, generic and master administration accounts must be stored in the IT Password vault

- Service accounts are the only accounts that are excluded from automatic password expiry to have passwords that do not expire and must have their passwords changed on request of the IT Manager
- All Service Account passwords must be complex (i.e. a mix of upper, lower, alpha, numeric, non-character) and at least 12 characters in length and generated using the password generate feature in the Dairy Australia password vault
- Local accounts (or non-Active Directory integrated) must not be created or used for any IT systems unless there is no other solution and only when approved by the IT Manager
- Any passwords stored in systems (e.g. connection strings, service account passwords, etc) must be encrypted and not visible without appropriate administrative access
- All systems must have their default passwords changed and details stored in the Dairy Australia IT password vault

3.3.1 Password protection standards

All passwords are to be treated as sensitive confidential Dairy Australia information and must not be shared with anyone, including Dairy Australia employees or individuals outside of Dairy Australia. The following standard and guidelines apply when using passwords within the Dairy Australia IT environment:

- Do not use the same password for the Dairy Australia accounts as for other non-Dairy Australia access (e.g. personal Internet or email account, banking, online shopping, etc.)
- Never share the Dairy Australia passwords with anyone, including but not limited to other staff (casual or permanent), IT support, administrative assistants, personal assistants, contractors, consultants, family or friends
- Never use another person's account details (username and password) to access a Dairy Australia IT system
- Where possible use biometric authentication methods provided by Dairy Australia (e.g. Windows Hello)
- Avoid using the same password in multiple systems or Web sites
- Never email a password to anyone
- Don't use your username as your password
- Don't use easily guessed passwords, such as 'password' or 'user'
- Do not choose passwords based upon details that may not be as confidential as you'd expect, such as your birth date, your phone number, or names of family members.
- Do not use words that can be found in the dictionary. Password-cracking tools freely available online often come with dictionary lists that will try thousands of common names and passwords. If you must use dictionary words, try adding a numeral to them, as well as punctuation at the beginning or end of the word (or both!)
- Avoid using simple adjacent keyboard combinations: For example, 'qwerty' and 'asdzxc' and '123456' are horrible passwords and are trivial to crack
- Use a Pass Phrase instead of a password - some of the easiest-to-remember passwords aren't words at all but collections of words that form a phrase or sentence, perhaps the opening sentence to your favourite novel, or the opening line to a good joke. Complexity is

nice, but length is key. Each character you add to a password or passphrase makes it an order of magnitude harder to attack via brute-force methods

- Ensure Multi-factor Authentication (MFA) is enabled on every system used – MFA will be enabled on all systems integrated with the Dairy Australia SSO system and any other systems that Dairy Australia provide where it's supported.
- Use a password manager that works as a browser extension and doesn't need software installed
- Don't store a list of passwords on a computer in plain text (e.g. Text file, OneNote, sticky note, etc). If a user must rely on written information for passwords then the most secure method for this is to create a list of every system required and next to each one write the login name and a clue that has meaning only for the user. This is discouraged though because if a password is forgotten, most systems will email details on how to reset it (assuming the user can remember which email address was used to sign up).

The following should not be used in passwords:

- Names of family, pets, friends, co-workers, fantasy characters, etc
- Computer terms and names, commands, sites, companies, hardware, software
- Words associated with the organisation such as 'DA', 'Dairy', 'Dairy Aust' or any derivation
- Birthdays and other personal information such as addresses and phone numbers
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc
- Any of the above spelled backwards
- Any of the above preceded or followed by a digit (e.g. secret1, 1secret)

Password cracking or guessing may be performed on a periodic or random basis by the IT Team or delegates. If a password is guessed or cracked during one of these scans, the user will be required to change their password immediately.

Any time using automated or manual methods the IT team may check against known data breaches to see if a password you use has been compromised - for example using https://haveibeenpwned.com/. If an account has potentially been compromised, the password will be required to be changed immediately.

3.4 Multi-Factor Authentication (MFA)

The following controls apply:

- All accounts that are synchronised to Azure AD will have Multi-Factor Authentication (MFA) enabled by default
- Only service accounts or the 'break glass' Office 365 administration accounts can be excluded from MFA and only with the approval of the IT Manager

3.5 Self-Service Password Reset (SSPR)

- Self-service password reset will be enabled for use on all user accounts
- Administrative and service accounts will not have Self-service password reset enabled.

4 Access Management

Any access provided to IT systems (both cloud and on-premises) must follow the Principle of Least Privilege (PoLP) and ensure that user accounts are given only those privileges required to perform intended functions or tasks.

All access must also be designed and managed around the Role Based Access Control (RBAC) principle and access controlled via Active Directory groups.

5 Single Sign on (SSO) and user provisioning

To ensure the integrity of data and control access, all IT systems (including cloud based and custom developed applications) must be integrated into the Dairy Australia SSO systems.

- For internal facing systems this is Microsoft Azure Active Directory
- For external facing systems this is Salesforce

Internal facing systems must also adhere to the IT standards for user provisioning and management. These standards are maintained by the IT Team and can be provided upon request.

Any exception to this can only be approved by the IT Manager.

6 Network Security

This section defines standards for connecting to Dairy Australia's corporate data network. These standards are designed to minimise the potential exposure to Dairy Australia from damages which may result from unauthorised use of the Dairy Australia resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, damage to critical Dairy Australia internal systems, etc.

All Dairy Australia networks will be

- protected by a firewall which will only allow required traffic in/out of the network
- Have colourless network ports implemented to automatically profile and segregate/isolate unauthorised devices

6.1 Connecting devices to the network

No device can be connected to the Dairy Australia data network (either within the office, or via a remote connection such as a VPN (virtual private network)) without written authorisation of the IT Manager unless it is supplied and approved by the IT Department.

The Dairy Australia network includes the physical network (ethernet), wireless network (WIFI) and remote access (VPN).

Examples of devices that are not authorised to be connected to the Dairy Australia network include but are not limited to:

- personal devices of any kind (laptop, mobile, tablet, printer, camera, etc) whether they are for personal use or required to complete business related tasks
- devices provided by, or used by consultants or contractors
- any device not supplied by the IT department.

Immediate removal and blocking of such devices can be made by IT or any Dairy Australia staff member and they are to immediately provide the device to the IT Team with a description of the observed use.

In the event an unauthorised device is removed by IT, or provided to IT by a staff member, Dairy Australia may request any data (Intellectual Property) on the device that can reasonably be deemed to be owned by Dairy Australia be removed before returning the device. The IT team may hold such devices until satisfied that a sufficient review of the contents of the device has occurred. A device can include but not be limited to a Laptop, USB stick or drive, smart phone, or tablet device (iPad).

6.2 Remote access

Secure remote access is strictly controlled and limited. Remote access to the Dairy Australia network can be facilitated in several ways:

- VPN – for Dairy Australia computers accessing the Dairy Australia network
- Remote Desktop (RDP) – for authorised staff, contractors and vendors to access a management server
- Just in time access (JiT) – direct access to servers managed by Microsoft Azure where a user needs to log onto Azure and request access which is approved and enabled/disabled automatically for the duration of the use.

The following apply to the above remote access methods:

- Access to the Dairy Australia VPN is restricted to devices approved by the IT Manager and authenticated with a certificate issued by the Dairy Australia Certificate Authority
- External RDP access must be approved by the IT Manager and only occur via the Dairy Australia jump box and is restricted to staff, contractors and vendors that need access to servers.
- JiT (Just in time access) can be provided to authorised support staff, vendors and contractors that need access to servers. Access by the IT Managed Services partner is allowed for all Level 2 and above support staff. Any other access must be approved by the IT Manager.

6.3 Physical network security

- Network ports will not be patched (connected) unless they are required to be used
- All vacant network points in publicly accessible areas will be locked out by using ethernet port locks to restrict the unauthorised use
- Ethernet cables in publicly accessible areas will be locked in using cable locks where possible. Where using a cable lock is not possible due to the device not supporting it, the situation will be reviewed to determine what other options are available.

6.4 Wireless network security

Dairy Australia provides corporate, BYOD and guest wireless network access (Wi-Fi) for use as required.

- All Dairy Australia provided devices will be configured to connect to the relevant Wi-Fi network automatically

- Connection to the corporate Wi-Fi network is managed by Dairy Australia issued certificates at a device level. Access to the corporate Wi-Fi is not configured or permitted using username and/or password.
- Connection to the BYOD network is integrated into Active Directory and only for use by authorised Dairy Australia employees and will adhere to the same account verification and lockout policies listed in section 3 Account Security.
- Dairy Australia users that have been provided with a Dairy Australia account are not permitted to use the guest Wi-Fi network
- Access to the Guest network requires the guest to register and be approved by a nominated Dairy Australia representative before the access is granted

7 Endpoint Protection

This section establishes a standard for implementation and use of Endpoint Protection (security software) and the frequency of change within Dairy Australia.

- Endpoints will be built using a secure configuration standard, which has been hardened to remove unnecessary functionality
- Endpoint protection (EPP) software must be installed on all supported devices (Windows & Apple Mac) including computers and servers
- EPP software will be automatically upgraded on computers on at least a monthly basis
- EPP rules, definitions and any other information required for operation and detection of threats will be updated on a daily (or as required) basis automatically
- The Dairy Australia Mobile Device Management (MDM) agent will be installed on all mobile (phone & tablet) devices accessing Dairy Australia IT systems

8 Access to IT systems from Mobile Devices

- All access to Dairy Australia IT systems will be managed by the Dairy Australia Mobile Device Management (MDM) system
- All Dairy Australia provided Mobile devices will be enrolled in the Dairy Australia Mobile Device Management (MDM) system and have appropriate security restrictions enforced including the ability to fully wipe or lock the device remotely
- Access from non-Dairy Australia provided mobile devices (phones & tablets) is permitted and will be controlled via Mobile Application Management (MAM) policies. These policies will enforce security requirements for the device and applications used to access Dairy Australia IT systems such as requiring a PIN, automatic screen lock, etc to appropriately protect the security of the Dairy Australia IT systems and data accesses from these devices

9

10 Email Protection

The following applies for protection of the Dairy Australia email system:

- All inbound and outbound email will be scanned for threats by the email security system

- Data loss prevention policies will alert users when they send an email that contains sensitive information - matching pre-defined rules managed by the vendor – including
    - Australia Financial Data
    - Australia Health Records Act (HRIP Act)
    - Australia Privacy Act
    - Australia Personally Identifiable Information (PII) Data
- URL rewriting (Safelink protection) will be implemented to ensure all links in emails are redirected to, and scanned by, the email security system before users access them

11 Web Security

The Dairy Australia web security system manages all outbound internet access from within the Dairy Australia network, or from a Dairy Australia managed computer.

The following applies:

- All Dairy Australia computers will have the web security agent (or applicable software) installed
- Any updates to the web security agent (or applicable software) will be deployed as soon as they are available from the vendor
- Website access via the Web security system can only be bypassed with approval of the IT Manager via the IT Change Management process
- All outbound web-based network traffic (e.g. HTTP & HTTPS) from the Dairy Australia network will be tunnelled directly to the web security system for transparent scanning (e.g. scanned automatically without needing to manually configure proxy settings)

12 Patching and vendor security updates

The following applies to patching and vendor security updates

- All routine patching will adhere to the Dairy Australia IT Change management process and be approved by the IT Manager (or delegate) as required
- Workstation operating system (OS) patching will occur monthly and will commence with a pilot group within one week of the updates being released by the vendor. The pilot group will test for less than one week, after which if there are no issues the updates will be deployed to all computers.
- Third-party software will be updated as part of the monthly patching on all workstation computers
- Server applications will be updated regularly as required to maintain the application at a vendor supported and recommended level and follow the IT change management process. Any critical security updates will be applied as soon as practical after advice from application vendors
- Computers will automatically enforce the installation of patches one week after they are released
- Critical security patches can be deployed out of cycle as soon as they are released if they are deemed to be required

- Server Windows operating system (OS) patching will occur monthly and will commence with a test group within one week of the updates being released by the vendor. This will be followed by all production servers one or two weeks later depending on the outcome of the test deployment.
- Network and hardware devices will be reviewed every three to six months for required updates and will be updated as required. Where a critical security update is recommended by the vendor, the device will be updated out of cycle.

12.1 Physical security

In addition to the physical network security requirements, the following will apply:

- IT Comms and storage rooms at Southbank are secured behind locked doors controlled by access cards
- Access is granted with approval of the IT Manager.

13 Security Incident Management

Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorised to access, unless these duties are within the scope of regular duties.

Security incidents from external sources include, but are not limited to, targeted phishing emails, data breaches or unauthorised access or hacking attempts.

Security incidents and breaches can be identified via a number of methods including but not limited to the following:

- Employees reporting any potential security breaches or security incidents to IT
- Third party IT managed services proactively monitoring the IT environment
- Automated systems such as Microsoft 365 Defender or the Crowdstrike Falcon service
- Reviews of audit and logging information in the IT environment

In addition, Intrusion Detection / Prevention System (IDS/IPS) will be implemented, with any alerts actioned to identify potential security incidents.

Any security incidents must be logged in the IT Service Desk and be managed by IT in line with the IT incident management and Cyber Security response processes maintained by IT. Major security incidents or near misses will also be recorded as a Dairy Australia incident.

Regular testing of the security incident management process will be performed, and any lessons incorporated into procedures and training materials.

14 Third Party Access

All third party access to DA IT systems must be approved by the IT Manager.

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
- procurement or development of any IT systems or functions.

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.

15 System Testing

Regular testing of the IT environment will be performed to determine whether there are any additional IT Security 'better practices' that can be implemented. This includes, but is not limited to, internal and external network vulnerability scans and internal and external penetration testing, review of access to determine whether it aligns with roles and responsibilities and review of system configurations.

16 Compliance and Assurance

The General Manager BOP must ensure appropriate monitoring compliance processes are in place for this Procedure. Any user non-compliance with the IT Security Policy and procedures may result in the immediate disabling of the account and could result in formal disciplinary action.

Breaches of this Procedure should be recorded as an incident.

Table 1 summarises the key compliance obligations in this Procedure which will be monitored and reported in the Irregularities Report.

Table 1: Key Compliance Obligations

Key Compliance Obligation	Relevant Control(s)	Monitoring Method(s)	Frequency
Account requests for consultants and guests must be approved by the relevant General Manager and the IT Manager, and a request submitted to the IT Service Desk.	The IT Service desk will not create an account unless approval is obtained by the relevant GM and the IT Manager. In addition, where an account for a non-staff member is created, the account is marked with an expiration date based on either a known end date, or an estimated duration that the account is required.	Service Desk account creation process Quarterly review of accounts to confirm they are valid	When a request to create an account is received. Quarterly
Relevant managers and HR notify the IT Service Desk that the user is leaving. In addition, Dairy Australia will generally suspend access for users on extended leave (e.g. > one month).	Accounts are regularly reviewed and accounts that are found to be inactive (e.g. expired, locked, not logged into for an extended period) will be disabled and after 30 days removed from the system if no longer required.	Quarterly review of unused accounts	Quarterly
Administrative accounts must be approved by the IT Manager before they are created.	The IT Service desk will not create an administration account unless approval is obtained from the IT Manager.	Service Desk account creation process Quarterly review of accounts to confirm they are valid	Ongoing Quarterly
Administrative access to any IT systems must be approved by the IT Manager or an approved delegate (e.g. technical owner of the application). This approval requirement cannot be delegated for core IT systems including Office 365, Active Directory, IT Password Vault, or any system where sensitive data is stored.	The IT Service desk will not provide administrative access unless approval is obtained from the IT Manager.	Service Desk account creation process Quarterly review of accounts to confirm they are valid	Ongoing Quarterly
All account passwords (e.g. user or administrative accounts) must have password expiry enabled and passwords will be required to be changed at a maximum every 90 days.	The Active Directory system where all user accounts are held utilises Active Directory Group Policy (GPO) to enforce this for all accounts.	The service desk review accounts on a quarterly basis to ensure no user accounts are set to bypass the password GPO.	Quarterly

Key Compliance Obligation	Relevant Control(s)	Monitoring Method(s)	Frequency
Regular testing of the IT environment will be performed to determine whether there are any additional IT security 'better practices' that can be implemented	IT Security testing	Any IT security testing is presented to ARMC and any recommendations and actions arising are reviewed and followed up until completed.	At minimum every two years
All accounts are required to have MFA enabled	The Azure Active Directory conditional access policies enforce MFA by default on all accounts. Accounts can only be excluded by being added to a specific exclusion group which is reviewed on a regular basis	Quarterly review of accounts to confirm they are valid	Quarterly

17 Roles and Responsibilities

The table below documents relevant roles and responsibilities:

Role	Responsibilities
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 • Must not in any way divulge, copy, release, sell, loan, alter or destroy any information • Must safeguard any physical key, ID card or computer/network account that enables access to Dairy Australia's information. This includes maintaining appropriate password creation and protection measures as set out in section 3.1. • Report any activities considered likely to compromise sensitive information to the relevant General Manager or to the IT Manager • Protect sensitive information even after leaving Dairy Australia. • Complete the IT Security training module on an annual basis • Complete any other IT security training as required
IT Manager	• Implement appropriate information security controls and processes to protect Dairy Australia from cyber security threats • Implement secure user access management for all Dairy Australia authorised users • Educate users on how to reduce the risks of cyber security incidents

Role	Responsibilities
	• 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
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 • procurement or development of any IT systems or functions 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

18 Review

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

19 Terms and Definitions

Term	Definition
Access control	Is the selective restriction of access to Dairy Australia's information

Term	Definition
Administrative access	Users of a system who have one or more of the following, and may include systems and database administrators: the ability to change key system configurations the ability to circumvent security measures access to data, files, and accounts used by other users, including backups and media special access for troubleshooting a system
Cyber Security	The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and / or defended against damage, unauthorised use or modification, or exploitation
Device	Can include but not be limited to a Laptop, USB stick or drive, smart phone, or tablet device (iPad).
Multi Factor Authentication (MFA)	Is an additional level of security for accounts. It is also known as two factor authentication where the user is required to verify they are the owner of the account being used to log in by using a secondary method of authentication (e.g. a text message with verification code) to verify their identity for a login or other transaction.
Password Passphrase	Is a word or string of characters used for user authentication to prove identity to gain access to a resource.
Security	Refers to the safety of Dairy Australia's data in relation to access control, authentication, physician and virtual security.
Sensitive Information	Information is considered sensitive if it can be damaging to Dairy Australia or its customers' reputation or market standing, or data classified as sensitive under the relevant privacy laws. Examples include privacy data, confidential data, Levy data, industry data or financial data (e.g. credit card numbers).
Single Sign On (SSO)	Single sign-on is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems. True single sign-on allows the user to log in once and access services without re-entering authentication factors