INFORMATION TECHNOLOGY ACCEPTABLE USE PROCEDURE

For internal Dairy Australia use and distribution only.

Once printed, this is an uncontrolled document.

Approved April 2023

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 following documents: • Acceptable use policy • Laptop, Desktop and Tablet Policy • Mobile Device Policy
03	GM BOP	April 2023	LT	April 2023	MD	May 2023	• Removed information relating to user accounts and account security that is duplicated from the IT security policy and procedure and replaced with reference to those documents • Updated privileged access section to refer to the IT security policy and procedure • Updated email section to include reference to encrypted data transfer requirements. • Updated MDM section to reflect changes from MobileIron to Microsoft Intune • Updated backup of data section to clarify only approved storage systems are allowed • Updated guest wifi to be approved by anyone in DA (sponsor) • Updated SaaS section to reference IT enterprise architecture

							• Updated File storage and sharing to be clearer that systems must be approved, added referenced to Microsoft 365, reflect same wording from the policy document, and sensitive data must be encrypted/protected when transferred • updated compliance section remove GM approval for guest accounts and updated monitoring for privileged access to include all core systems, not just Active Directory • adjusted wording in numerous sections to clarify meanings and standardise references (eg Dairy Australia IT) • - Added clarification in roles and responsibilities that HR is also responsible for monitoring training module
Document Steward							**IT Manager**
Document Owner							**General Manager BOP**

Related Documents
IT Acceptable Use Policy
IT Security Policy
IT Security Procedure
Code of Conduct
Social Media Policy
Social Media Procedure
Review Requirements
This document is due for review in April 2024 by the General Manager BOP
Controlled Document Location
https://dairyaustralia.sharepoint.com/SitePages/documenthub.aspx

Contents

INFORMATION TECHNOLOGY ACCEPTABLE USE PROCEDURE

1 Purpose

The purpose of this procedure is to document the acceptable and non-acceptable uses of Dairy Australia's information technology resources to ensure that these are used in a secure, legal, ethical and responsible manner.

2 Scope

This procedure applies to all Dairy Australia employees, both Southbank and regionally based, including fixed term, casual, Dairy Australia directors and contractors and all parties who access Dairy Australia's information technology infrastructure, hereinafter referred to users.

This procedure must be read in conjunction with the *Information Technology Acceptable Use Policy (AUP),* the *Information Technology Security Policy* and the *Information Technology Security Procedure.*

3 General Use and Ownership

While Dairy Australia's Information Technology (IT) Department will provide a reasonable level of security and privacy, users should be aware that the data they create on Dairy Australia's Information Systems remains the property of Dairy Australia. Because of the need to protect Dairy Australia's IT systems, electronic assets and data, Dairy Australia cannot guarantee the confidentiality of personal information stored on any of its IT systems or devices.

Users are responsible for exercising good judgment regarding the reasonableness of personal use of Dairy Australia's Information Systems. When in doubt users should consult their manager, General Manager or the IT Manager.

During normal use of the Dairy Australia IT systems, users may have their activities monitored. Dairy Australia reserves the right to audit networks and systems which form part of Dairy Australia's Information Systems on a periodic basis to ensure compliance with the *IT Acceptable Use Policy and Procedure.*

4 Security and Proprietary Information

Information contained on network drives, file storage and other IT systems where possible should be classified and treated as either confidential or not confidential. Examples of confidential information include, but are not limited to, company confidential documents, corporate strategies, industry data, levy data, customer lists, research data and information defined under the Privacy act. Users should take all necessary steps to prevent unauthorised access to this information.

Emails by users from a Dairy Australia provided email address will have a Dairy Australia (or equivalent) authorised disclaimer automatically appended. Users should not include their own disclaimer unless approved by the Legal Manager and IT Manager.

Postings by users to any social media site must align with the *Social Media Policies* and the *Social Media Procedures*.

Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, trojans, suspect code or attempts to obtain information (e.g. phishing). Dairy Australia takes no responsibility for any personal data stored on equipment provided as part of Dairy Australia's IT systems. Such data will not form part of Dairy Australia's backup or recovery processes and will not be migrated from one device to another by Dairy Australia's IT Department as part of an upgrade or repair to a device.

Users must ensure they are familiar with the IT Cyber Security guidelines (published on the IT support page on Dairy Hub) and ensure that any guidance provided by the Dairy Australia IT team is followed when required. These guidelines support and complement the IT Acceptable Use Policy and Procedure and must be read in conjunction with these documents.

Dairy Australia's corporate data copied from corporate servers or approved data storage locations for remote or offline use must only be stored on encrypted devices or Dairy Australia computers. Dairy Australia's IT Department will not be held accountable for the recovery of corporate data not stored appropriately and will report such storage as a breach of the IT Acceptable Use policy.

5 IT Systems Usage

IT systems usage covers the use of all IT systems including but not limited to

- Email
- Internet access
- Dairy Australia owned or operated websites
- File storage locations (network or cloud based)
- IT equipment
- IT provided software

Users must not knowingly use or attempt to use Dairy Australia's Information Technology resources for unlawful, offensive or otherwise improper activities including but not limited to:

- harming (whether physically, financially or otherwise) another person or company
- damaging another person's property or services, networks or facilities
- contravening any law or regulation
- placing Dairy Australia in contravention (or at risk of being in contravention) of any law or regulation
- contacting a minor who is not known to the user, without the consent of that minor's parent or guardian
- enabling a minor to obtain access to inappropriate material
- harassing, menacing, or stalking any person
- unlawfully discriminating against any person

- unlawfully vilifying any person
- storing, publishing or disseminating any obscene material (including child pornography)
- publishing or disseminating any defamatory material
- infringing any person's legal rights, including rights relating to intellectual property, fair trading, confidential information and trade secrets
- contravening any law relating to privacy
- engaging in the practice known as 'spamming' or altering the contents of an electronic message for the purpose of hiding, obscuring or deleting the source of the message or making the message appear to come from someone other than you
- creating or knowingly disseminating any virus, trojan, worm, cancelbot, time bomb, hacking tool, or other harmful component
- granting any person unauthorized access to or control over any service, network, facility or equipment
- engaging in a denial of service attack or the practice known as 'flooding'
- defeating any security measure or usage limit imposed by Dairy Australia

The following activities are strictly prohibited:

- violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of 'pirated' or other software products that are not appropriately licensed for use by Dairy Australia
- unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Dairy Australia or the end user does not have an active license
- exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The IT Manager should be consulted prior to export of any material that is in question.
- introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan Horses, e-mail bombs, etc.)
- revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home
- using a Dairy Australia computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws
- making fraudulent offers of products, items, or services originating from any Dairy Australia account
- making statements about warranty, expressly or implied, unless it is a part of normal job duties
- effecting security breaches or disruptions of network communication. 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
- port scanning or security scanning is expressly prohibited unless prior notification the IT Manager is made and approved

- executing any form of network monitoring which will intercept data not intended for the employee, unless this activity is a part of the employee's normal job/duty
- circumventing user authentication or security of any computer, network or account
- interfering with or denying service to any user (for example, denial of service attack)
- using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet
- providing information about, or lists of, Dairy Australia employees, contractors or suppliers to parties outside Dairy Australia

6 Personal Use

Reasonable non-commercial use of Dairy Australia's computers, email and Internet systems is acceptable, but all use must be in accordance with the IT Acceptable Usage Policy and IT Acceptable Usage Procedure and any use may be monitored.

7 Monitoring

Users should have no expectation of privacy in anything they store, send or receive on Dairy Australia's IT systems. Dairy Australia may monitor activity on any IT systems without prior notice. Each user of Dairy Australia's IT systems must also play their role in remaining vigilant in ensuring that the system is not misused by alerting the IT Manager as soon as they become aware of any misuse or security concerns.

8 User Accounts

Accounts, passwords and any other forms of access credentials for use on Dairy Australia IT systems must be created and managed in accordance with the IT Security Policy and IT Security Procedure.

Providing user account details to another user (including IT support) or using another user's account details to log into any IT system for any purpose is strictly prohibited unless approved by the IT Manager. Where access to another staff member's data or systems is required appropriate delegation, sharing or individual access must be setup for the required user.

8.1 Privileged access

Where a higher level of access is required to a system to perform administrative functions a separate Administration account will be provided to relevant staff in accordance with the IT Security Policy and IT Security Procedure. Administrative accounts must not be used for day to day activities under any circumstances.

8.2 Suspension, review and termination of accounts

When a user leaves Dairy Australia, it is the responsibility of the line manager to ensure that the IT Service Desk has been notified that the user is leaving. As a backup, HR will also notify the IT Service Desk once they become aware of a staff member resigning.

Dairy Australia will generally suspend access for users on extended leave (e.g. >one month). In addition, at the request of the relevant General Manager, access to IT systems may be suspended for a shorter period if they feel that this will assist the staff member with disconnecting from Dairy Australia and coming back to work after a leave period fully refreshed.

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.

9 Internet Access

Internet access is provided to all Dairy Australia users to perform their roles within Dairy Australia. Dairy Australia employs a third-party Web Security system to monitor all Internet traffic and block access to unauthorised, illegal or content deemed to not be required for use within Dairy Australia.

If websites or content are incorrectly blocked a request can be made to the IT Service Desk to have the site or content reclassified with the third-party system.

10 Email

When emails are sent using the Dairy Australia's email system it is quite rightly perceived by the general public and others that view the message as an official communication from Dairy Australia.

The section below provides guidance on the correct use of the corporate email system by Dairy Australia's staff.

10.1 Prohibited use

In addition to the guidelines in the Acceptable Usage Policy and IT Systems Usage section of this procedure, sensitive information such as privacy data, confidential data, Levy data, industry data or financial data (e.g. credit card numbers) must only be distributed via Dairy Australia IT approved encrypted transfer methods and not be distributed without approval to ensure compliance with relevant laws and industry standards such as payment card industry compliance (PCI).

Dairy Australia employs a third-party Security systems to log and monitor all data transfers and email traffic, and rules are in place to block and alert users and IT administrators when sensitive or inappropriate data is sent or transferred.

If users receive any email that is in breach of the IT Acceptable Usage Policy or this procedure in their Dairy Australia email account, the email in question should be reported to that person's supervisor and the IT Manager immediately.

10.2 Email account management

The following standards apply to email accounts:

- All Dairy Australia staff will receive a 100GB mailbox limit
- All non-Dairy Australia staff who require use of the email system will receive a 50GB mailbox limit
- All mail older than two years will be automatically moved to an online archive
- Legal hold and journaling (e.g. recording all communications for use in the email retention or archival strategy) will be used to track and store all email sent/received through the Dairy Australia IT systems
- Creation of .PST files (local archives) is prohibited. All email should be stored in mailboxes or online archives, and access to email on personal devices will only be approved for devices using the Dairy Australia managed Mobile Device Management (MDM) Software. Such management will facilitate Dairy Australia in protecting its Intellectual Property in the event of device loss or threat.
- Emails stored in the deleted items may be removed in the event that Microsoft Office 365 or Dairy Australia policies change. The deleted items folder should never be used for the storage of emails.

11 Mobile Device Management

Dairy Australia allows access to corporate Dairy Australia systems (including Office 365) on mobile devices only via apps that are compatible with Mobile Application Management (MAM) and Mobile Device Management (MDM) software. This solution allows Dairy Australia to protect its Intellectual Property in the event of device loss or threat.

Any device (personal or Dairy Australia issued) that has access to Dairy Australia systems which is lost or suspected of being lost or stolen must be reported to Dairy Australia IT as soon as practically possible. Dairy Australia IT may, based on the information provided, opt to block and erase all Dairy Australia information (including files and email) from the mobile device as the best way to ensure its security in this compromised context. The MDM does not access personal data on a device,

Where a device is provided by Dairy Australia (corporate owned) all data including personal data maybe erased if a device is lost or stolen. Where a device is being used as a BYOD (bring your own device) only Dairy Australia data and apps will be erased if a device is lost or stolen

12 IT Hardware

IT Hardware including computers (laptop or desktop), peripherals (screens, mice, keyboards, etc) and any other devices are provided for the sole purpose of conducting Dairy Australia activities. The use of such devices for reasonable personal use is acceptable, however Dairy Australia does not allow the installation of unauthorised or inappropriate software on any device. Under no circumstances are these devices to be used for activities for any commercial or non-commercial business other than that conducted for Dairy Australia.

Dairy Australia utilises applications to monitor use of IT equipment and control application installation and usage. Any attempt to circumvent or avoid the IT management applications or security policies is prohibited and could result in disciplinary action.

The type of device provided to an individual will be decided by the IT Manager, the General Manager BOP or the Managing Director, based on a demonstrated business need. At all times the device remains the property of Dairy Australia.

Managers are responsible for ensuring the IT Service Desk is informed of any staff member exiting the business. This is to allow IT time to remove access to IT systems in line with the termination. The Manager is responsible for returning the individual's IT devices to IT. Final payment of salary for the departing staff member will only occur after HR have confirmed that all IT hardware has been returned to the IT team.

12.1 Securing IT hardware

IT hardware must be kept secure at all times whether in the office, in transit or at home. Hardware should never be left in a visible location, whether that be an office, car or elsewhere, or overnight in a locked car.

Laptops that are not secured may be confiscated by the IT team at any time and without warning. Securing hardware means not leaving it in an open office overnight and can be as simple as placing it out of sight in a locked desk drawer. Individuals will then be required to justify why their device was not secured. This will be done in writing to their General Manager, copying in the IT Manager. Hardware will not be returned until the IT Manager receives written approval from the individual's General Manager.

Ongoing failure to properly secure devices covered by this policy could result in disciplinary action.

12.2 Purchase and replacement of devices

All IT hardware purchases must follow the Delegation of Authority and be approved by the IT Manager. The IT Manager will have the final say on the specifications and type of hardware to ensure consistency, compatibility and security of Dairy Australia's IT systems.

Dairy Australia will generally replace its desktop/laptop hardware once every three to five years.

The purchase of any technology hardware tool not pre-approved or arranged by the IT Manager may result in payment cancelled by Finance or seeking reimbursement from staff member or having the device permanently removed from use by the IT Manager.

The General Manager BOP has the discretion to enforce any of the above steps.

12.3 Loss and replacement

If a device is lost, it must be reported to the IT team immediately to enable appropriate action to be taken. Dairy Australia takes no responsibility for data loss of any kind on the device where the data is stored outside the recommended and backed up storage locations. Refer to section 12.4 for information on recommended storage locations and the responsibilities relating to recovery of data not stored in these locations.

In the event of loss or damage, a written incident report must be completed and supplied to the IT Manager, relevant line manager and General Manager within two (working) days of the incident. This report must document how and where the loss or damage occurred, what steps were taken to avoid the loss/damage and any third parties that were involved (names of hotels, individuals, etc.). Where appropriate a police report is to be provided.

Repairable damage not covered under warranty will be repaired at Dairy Australia's cost. If a second repair is requested within a two-year period, General Manager BOP approval is required for the repair to be at Dairy Australia's cost. The General Manager BOP will decide whether the

repair will be funded by the department budget of the employee or by the user. If more than two repairs are requested in a three-year period, the cost for this and subsequent repairs will be recovered from the user and may result in disciplinary action.

In most instances the unit cost of IT hardware is less than $5,000 which is below the insurance excess, therefore Dairy Australia does not claim such items on insurance and the full replacement cost would need to be recovered for items not covered by insurance.

12.4 Backup of data

All Dairy Australia data must only be stored in storage locations approved by Dairy Australia IT that are backed up. Refer to section 17 File Storage and Sharing for information on recommended file storage locations.

Data stored outside the recommended storage locations or peripheral USB drives are not in any way supported or backed up by Dairy Australia. As such, users must ensure that all Dairy Australia related data is only stored in recommended and backed up storage locations to avoid data loss. Users are fully accountable for any Dairy Australia data loss and the time to recover/recreate this data if not stored in the recommended locations. Dairy Australia IT will facilitate assistance with such a task if it is approved and required.

Replacement of any lost data may also be at the user's expense to recover or recreate.

12.5 Device security

Laptop/desktop devices must be locked via a password when unattended or unused for any time. Dairy Australia will enforce such a policy on to devices via the IT Management systems where possible. In addition to the automated screen timeout on all computers, users should proactively lock their computers using the screen lock option. (WINDOWS + L).

Mobile devices and apps connected to the Dairy Australia systems must have a screen timeout and appropriate security to unlock the screen (e.g. PIN, biometric ID, or other). The MDM solution will enforce this and in situations where the device does not meet these requirements access to Dairy Australia systems from the mobile device may be automatically blocked or removed.

12.6 Hardware destruction

At what is deemed to be the end of useful life of any device, or in line with the replacement cycle, IT will arrange for the destruction and secure wipe of all Dairy Australia data on any device. This will include the removal of any applications licensed to Dairy Australia as well as all intellectual property.

Dairy Australia will, based on the age of the hardware, attempt to sell the hardware for a reasonable return or seek to have the device disposed of in an environmentally friendly way to ensure compliance with all applicable laws relating to e-waste disposal.

The option may be extended for staff to purchase hardware due for disposal if they are prepared to match or exceed the best price that Dairy Australia can reasonably expect to achieve selling the device via commercial means. All data and Dairy Australia owned software will be removed before any device is sold to a staff member. Any hardware sold to staff is sold 'as-is' and without warranty or support.

13 Bring your own device (BYOD)

Dairy Australia has multiple data networks including a Corporate, BYOD and Guest networks.

Dairy Australia does not support or allow BYO devices to be connected to the Dairy Australia corporate network. Where there is a need for a device to be used for corporate use it must be procured and supplied in line with section 12 IT Hardware of this document.

Users are permitted to connect a maximum of one personal mobile device (phone or tablet) to the Dairy Australia BYOD (bring your own device) network for the purposes of Internet access. Access to IT systems on the internal Dairy Australia network are not permitted and actively blocked from this network. Instructions on how to connect to the BYOD network can be found in the IT Knowledgebase.

14 Network

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

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

In addition to the corporate data network, Dairy Australia also provide network connectivity for other users such as guest access and staff BYOD which are outlined separately in procedure.

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

- 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 (include but not be limited to a Laptop, smart phone, or tablet device (iPad)).

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.

Under no circumstances are Dairy Australia staff to use their account details to connect or log anyone else (staff member, user, consultant, contractor, external guest, etc) onto the Dairy Australia network.

Exceptions other than those listed in section 13 Bring your own device (BYOD) must be approved by the IT Manager.

14.1 Guest network

Dairy Australia provides a Guest network that can be accessed both via physical connection (ethernet cable) or via the Guest Wi-Fi network.

Access to the Guest network requires the guest to request access via the captive portal once they have connected and for that request to be approved by a Dairy Australia staff member (sponsor) before the access is granted.

Dairy Australia users that have been provided with a Dairy Australia account are not permitted to use the guest WIFI network.

15 IT Software and Software as a Service

A Standard Operating Environment (SOE) is provided on all Dairy Australia issued computers. This SOE is updated regularly, and restrictions are in place the ensure the security and integrity of the Dairy Australia IT systems.

All software procurement, whether paid, free, cloud based, physical or otherwise must be performed in accordance with the Delegations of Authority and authorised by the IT Manager.

15.1 Software installations

A list of standard software available for installation on the SOE is maintained by IT and requests can be made for software to be procured and/or installed via the IT Service Desk. Where a license is required for a software installation, a sufficient business justification will also be required for the software to be installed on a user's computer.

Additional licensing for software specific to a business unit or group will be at the expense of the relevant department budget. Software licensing for applications provided across multiple groups will generally be covered in the IT Budget, however some exceptions may exist for specialist software and such situations will be evaluated at the time of the request.

Software, whether new or existing, can only be installed by the IT Team. Where new software outside of the SOE is required a sufficient business justification will need to be provided and approved in writing by the IT Manager. Before the new software is installed, the IT Team must be confident that no like software already exists within Dairy Australia, in which case the requester will also be asked to justify why the existing software does not meet their needs. If the existing software meets the majority or more of their needs this will be the software installed so that Dairy Australia can leverage the existing investments where possible and standardise on training and support processes. In addition, for new software the IT Team will need to ensure that the software does not jeopardise the security, speed and stability of the SOE, the network or violate any Dairy Australia policy, by carrying out its own testing.

Any software, regardless of it being existing, an upgrade or new, may not be installed if as part of the installation or configuration process, changes to Server or Desktop Operating systems are required that do not meet Dairy Australia IT standards or security requirements.

15.2 Software as a service

Software as a Service (SaaS) is a common description for cloud or internet-based software that does not need installation on a computer.

SaaS solutions such as personal webmail, banking, or systems provided by vendors/consultants in the course of providing services to Dairy Australia are permitted to be used without IT approval.

16 Saas Solutions

Where SaaS solutions (cloud based software) are to be implemented and used within Dairy Australia they must be reviewed and approved by the IT Manager and adhere to Dairy Australia IT standards and security requirements. Systems that fail to adhere to standard or security requirements or do not adhere to the IT enterprise architecture model must not be used.

17 File Storage and Sharing

Users must ensure that all data is stored and shared using only systems approved and provided by Dairy Australia IT. Storage of Dairy Australia data on non-Dairy Australia devices, or non-approved cloud storage services is prohibited without prior approval from the IT Manager.

The current list of approved systems is maintained in the IT Knowledgebase and regularly updated as required. The locations include but may not be limited to:

- Network Drives (eg I, M, S, etc)
- Dairy Australia Microsoft Outlook Email (encrypted email for sensitive information)
- Dairy Australia Microsoft OneDrive (not personal OneDrive)
- Dairy Australia Microsoft Teams (not personal Teams) including Sharepoint and any other Microsoft 365 systems
- TRIM (or equivalent Dairy Australia provided document management system)

Storing Dairy Australia files in personal file storage systems or accounts is strictly prohibited. This includes but not limited to systems such as personal computers, Dropbox, Google Drive, and other online storage systems not explicitly provided by IT. Personal subscriptions, or subscriptions taken out by Dairy Australia users without IT approval are not permitted.

Dairy Australia files must not be synchronised to or stored on non-Dairy Australia computers. Access to Dairy Australia cloud based file storage systems (eg Microsoft 365) from non-Dairy Australia computers is allowed via the web-based interfaces provided (e.g. webmail, Microsoft 365) and data should not be downloaded to non-Dairy Australia computers.

Sharing of sensitive data via unencrypted email or other unencrypted transfer methods is prohibited. Sharing of sensitive data must be approved by the owner of the data and performed using an encrypted or password protected transfer method that adheres to the IT Security Policy and Procedure.

Documents that are designed for public audience (eg presentations) are not classified as sensitive and can be transferred via USB devices, or shared via other means as required.

18 Compliance and Assurance

The General Manager BOP must ensure appropriate monitoring compliance processes are in place for this Procedure. Any user's non-compliance with the IT Acceptable Use Policy and Procedures may result in suspension of access to Dairy Australia's IT resource 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
Dairy Australia employees are aware of and understand the key requirements of the IT AUP Policy and Procedure	Training is provided to all employees annually and to new employees at induction	HR generate overdue training reports and forward to Leadership Team for actioning	Monthly
All IT purchases adhere to the Delegations of Authority and authorised by the IT Manager	The purchase of any technology hardware tool not pre-approved or arranged by the IT Manager may result in payment cancelled by Finance or seeking reimbursement from staff member or having the device permanently removed from use by the IT Manager	The Financial Controller reviews all invoices before payment is made. IT purchases which have not been authorised by the IT Manager are not paid until authorisation is obtained.	Twice a month
Account requests for consultants and guests must be approved by 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 from 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

Managers are responsible for informing the IT Service Desk of any staff member exiting the business and for returning the individual's IT devices to IT	Final payment of salary for the departing staff member will only occur after HR have confirmed that all IT hardware has been returned to the IT team.	n/a	As staff member exits
Users must not use the internet to access unauthorised or illegal content.	Dairy Australia employs a third-party Web Security system to monitor all Internet traffic and block access to unauthorised, illegal or content deemed to not be required for use within Dairy Australia	Web security system rules to block inappropriate content	Ongoing and whenever usage information is requested
Sensitive information such as privacy data, confidential data, or financial data (e.g. credit card numbers) must not be distributed via any means without approval to ensure compliance with relevant laws and industry standards such as payment card industry compliance (PCI).	Dairy Australia employs a third-party Email Security system to log and monitor all email traffic and rules are in place to block and alert users and log details when financial details are sent via email	Data leakage rules in Office 365	Ongoing
Creation of .PST files (local archives) is prohibited.	The Standard Operating Environment (SOE) has restrictions that prevent creation of PST files.	The IT Standard Operating Environment (SOE) restrictions prevent users from creating or updating PST files.	Ongoing
Users must not install unauthorised or inappropriate software on any device.	Dairy Australia utilises applications to monitor use of IT equipment and control application installation and usage. In addition, the Standard Operating Environment (SOE) has restrictions that prevent applications	The IT Standard Operating Environment (SOE) restrictions and application whitelisting prevent users from installing applications.	Ongoing

	from being installed unless performed by IT.		
Mobile devices connected to the Dairy Australia systems must have a screen timeout and appropriate security to unlock the screen and/or app (e.g. PIN, biometric ID, or other).	The MDM solution enforces this and in situations where the device does not meet these requirements access to Dairy Australia systems from the mobile device may be automatically blocked or removed.	MDM policies prohibit use of the DA systems from mobile devices without these settings configured.	Ongoing
Where a higher level of access is required to a system to perform administrative functions a separate Administration account will be provided to relevant staff. These administrative accounts must not be used for day to day activities under any circumstances	IT Service desk will not provide elevated access unless approval is obtained from the IT Manager. Approval will not be provided by the IT Manager unless it's required, appropriate and an Admin account is being used.	Service Desk account and access management processes Quarterly review of privledged account access across core systems including AD, Office 365, finance and HR systems.	When a request to create an account or provide elevated access to a system is received Quarterly

19 Roles and Responsibilities

The table below documents relevant roles and responsibilities:

Role	Responsibilities
Dairy Australia information technology users	• Are responsible for all activities originating from accounts and devices provided by Dairy Australia • Use Dairy Australia's IT resources in accordance with this procedure including appropriately securing any IT accounts and devices provided to prevent unauthorised use, theft or loss • Report any activities considered likely to breach this procedure to the relevant Manager, General Manager or to the IT Manager
IT Manager	• Implement appropriate information security controls and processes
Managing Director / General Managers / Regional Managers	• Ensure the IT Acceptable Use Policy and Procedure are implemented within area of control • Ensure appropriate action is taken when the IT Acceptable Use 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 The Agreement must 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 Acceptable Use Policy and Procedures • Ensure all employees and contractors review and acknowledge the IT Acceptable Use 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

20 Review

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

21 Terms and Definitions

Term	Definition
User	A person who has been granted access to all or part Dairy Australia's information infrastructure by a responsible officer
Bring Your Own Device (BYOD)	User's personal mobile device, not a Dairy Australia provided device
Email	The electronic transmission of information through an email protocol of any kind. Email clients include Microsoft Outlook and any webmail system such as Gmail, yahoo, outlook.com, etc
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).