Acceptable Use of Information Systems Policy

We Always Do The Right Thing

At Woolworths Group ("Woolworths") we aim to be Australia and New Zealand's **most trusted brand**. **Strong customer trust** helps Woolworths build, attract and retain customers, maintain a reputation for providing valuable products and services.

A breach of customer trust can result in harmful business consequences that can have a lasting effect and can take years to recover from. **Woolworths can grow customer trust by** respecting the trust customers place in us and through demonstrating we are doing everything possible to protect the information of our customers, Team Members and organisation.

This **Acceptable Use of Information Systems Policy** ("Policy") applies to any employee, contractor and/or third party ("Team Members") within Woolworths who is authorised to access any Woolworths' information and systems, including team members working in support offices, stores, distribution centres, working remotely or whilst travelling overseas.

It is your responsibility to:

1. Read the Policy
Make sure you have read this Policy. If there is anything you are unclear about, ask your Line Manager.

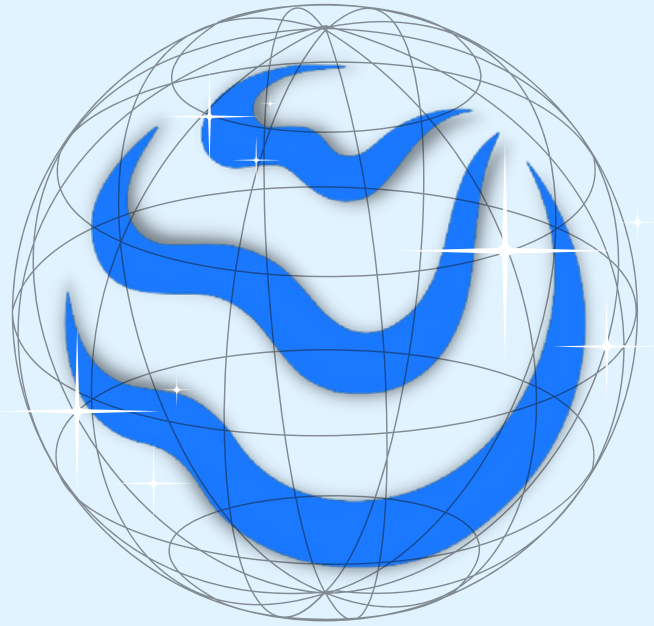
2. Agree to the Policy
You must acknowledge that you understand and agree to abide by the responsibilities set out in this Policy.

3. Follow the Policy
All Team Members within Woolworths are responsible and accountable for their own security behaviours.

Line Managers are responsible for ensuring direct reports have read, agreed and follow this Policy.

In addition, all Team Members must abide by the Enterprise Cyber Security Policy.

For more information and resources about securing your technology and staying safe online, visit the Woolworths Cyber Security Website.



Protect Woolworths' Information

Protect Woolworths' customers, team members and business information from misuse and loss. Information can be stored and shared in many different ways, including but not limited to; hard copy paper documents, computer files, emails, chat, videos, photographs, and device screens. Take care and be vigilant when storing and sharing information regardless of its format.

It is your responsibility to:

❑ Only collect, use, store and disclose Woolworths' information that is required for your role. Material created, sent, received, copied or stored on behalf of Woolworths is company property.

❑ Protect Woolworths' information according to 4 classifications; Public, Internal, Confidential and Restricted Information (as outlined in the Data Classification Standard).

❑ Treat Woolworths information in accordance with the Woolworths Group Data Principles.

❑ Never share or provide access to Restricted, Confidential or Internal Woolworths Group Information to individuals or Team members who have not been given explicit approval to view the information.

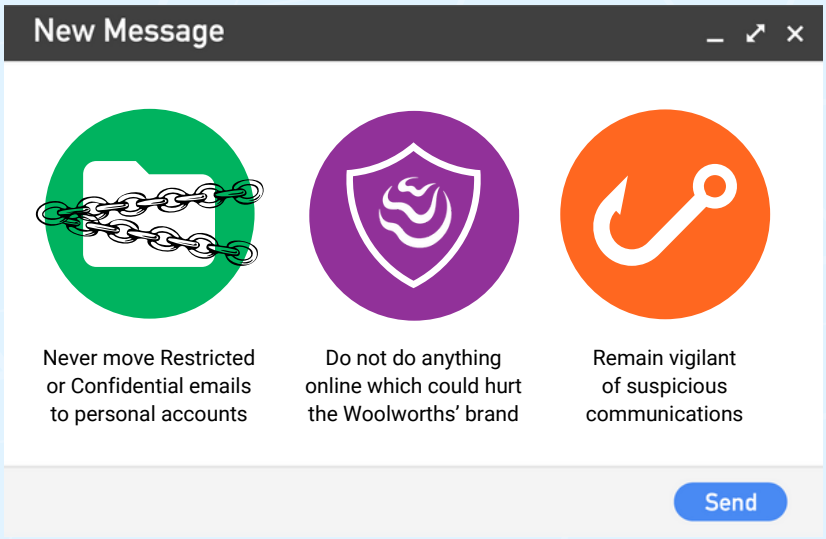
❑ Never send or store Woolworths Restricted or Confidential Information such as personal information, credit card details and cardholder data, employee salary and sales data, unless it is part of an authorised business process or activity that is compliant with Cyber Security Standards.

❑ Ensure hard copies of Restricted, Confidential and Internal Information are stored securely at all times and especially when unattended.

❑ Ensure whiteboards, jamboards and presentation aids are erased or securely stored at the end of a meeting.

❑ Ensure Customer information is only used for the purpose for which it is collected.

❑ Ensure any incidents, related to unintentional disclosure, loss or theft of customers' or employees' personal information (including but not limited to email address, phone number, physical address and date of birth) are reported to the Incident Management Centre (IMC) immediately on **1800 008 584** (Australia) or **0800 501 801** (New Zealand).



Report all suspicious communications to **hoax@woolworths.com.au**, **hoax@countdown.co.nz** or simply use the **Phish Reporter button** in your Gmail toolbar.

Use Email and Internet Safely

You must ensure you:

❑ Remain vigilant of suspicious communications that may:

- Create a sense of urgency
- Contain attachments you weren't expecting
- Are from people or organisations that don't usually contact you
- Request personal or sensitive information

❑ Do not use Woolworths email for the following purposes:

- Sending unencrypted Restricted or Confidential information
- Conducting non-Woolworths related commercial activities
- Creation or distribution of 'junk', 'chain' or 'spam' mail
- Subscribe to non-business related / personal services (for example, DropBox, Pokemon Go, TikTok etc).

❑ Corporate and personal accounts must be kept separate. Never move Restricted, Confidential or Internal information between corporate and personal accounts.

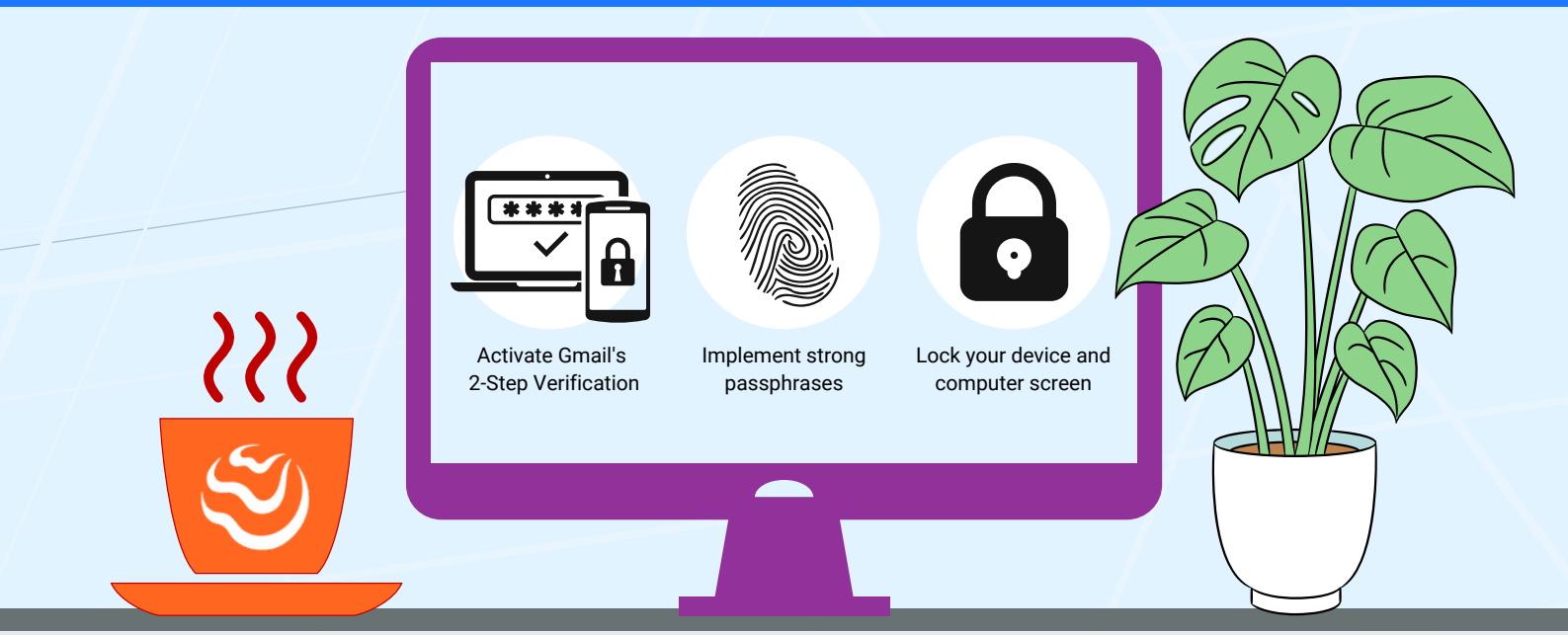
❑ Do not use Woolworths Internet for accessing, creating, downloading, retrieving, sending and forwarding material that is: illegal, pornographic, negative material that depicts race, sex or religion, derogatory or slanderous material or material in breach of copyright.

❑ Only install and use approved applications and extensions on your work profile. Unauthorised applications and extensions will be blocked.

❑ Never perform any action using Woolworths email and Internet which could bring the Woolworths brand and reputation into disrepute.

❑ Only use Woolworths approved systems and services for transferring and storing Restricted or Confidential information. Contact Cyber Security for guidance on using applications managed by external parties (for example cloud services).

Note: The Woolworths Group Cyber Security Team has oversight of the information accessed using Woolworths resources and devices. Logs may be generated, examined and monitored.



Manage Systems and Information Access

You must ensure you:

❑ Never share your Woolworths account details or passwords with anyone else.

❑ Activate 2-Step Verification on your Woolworths Gmail account.

❑ Implement strong passphrases on all devices and accounts which access Woolworths' systems and information. Passphrases are a combination of words that mean something to you and contain spaces in between the words, for example "I love 2 read policies!".
Passphrases should:

- Be 8 or more characters in length.
- Avoid using words that contain personal information (for example, first name, last name, date of birth).
- Avoid using common words (for example, password, welcome, woolworths, 123456).

❑ Where single sign-on is not available, ensure your passphrases are unique across your different accounts as the compromise of one account could cascade to the compromise of all your accounts with the same password. A password manager (for example, LastPass) can help you with this.

❑ Change the passphrases on your accounts:

- Every 60 days on all accounts with privileged access.
- Every 90 days for accounts or systems in the cardholder data environment in compliance with Payment Card Industry (PCI) standards.
- Every 365 days for service accounts.

❑ Never share a software licence with other team members. This includes sharing the licence key, username or password with others, or by using the licence through a shared account with other team members.

❑ Only use the systems access appropriate to your current job role. Privileged accounts hold great responsibility and can be revoked at any time by the Woolworths Cyber Security Team.

❑ Review access to systems at least annually and when team members transfer between roles.

❑ Remove access to systems from team members who leave the organisation. This includes requesting suspension of any privileged access on or before a team member's last working day.

Staying Safe while Working Remotely

Be aware of what you share. Ensure your workstation is tidy and secure, as to not let other individuals access the information stored in and around your device or workspace.

Stay vigilant and:

❑ Be mindful of and review your obligations under the Woolworths Technology Handbook, when working remotely.

❑ Avoid working in public places (for example coffee shops) where individuals could view or access the information stored on your device(s).

❑ Use secure, password protected wi-fi or your phone wi-fi hotspot to connect securely on the go. Avoid using free public wi-fi offered in shopping malls and restaurants.

❑ Continue using the communication platforms and tools provided by Woolworths (for example, your Google Mail, Chat, Meeting and Currents), not unprotected public platforms like WhatsApp or Zoom where possible.

❑ Never leave your portable devices unlocked or unattended. Leaving your device unlocked and unattended gives anyone the opportunity to gain access to the information stored on your device and could potentially lead to brand and reputational damage should the information fall into the wrong hands.

❑ Contact the Tech Centre for guidelines about keeping devices safe, while working remotely.

❑ Immediately report any Woolworths' device loss to your Line Manager, and to the IT Tech Centre or IT Service Desk so that the device can be remotely wiped.

Secure your Devices

Ensure that your devices comply with Woolworths standards and usage guidelines, at all times.

It is up to you to:

❑ Secure Woolworths' IT equipment at all times (for example, radio frequency guns, store iPads/ tablet devices, laptops, desktops).

❑ Lock the screen of your device when it is not in use, to prevent other individuals gaining access to the information stored on your device.

❑ The use of a personal device for work purposes is a privilege and it is essential that the device is secure. If you are using your own device to connect to the Woolworths network and work accounts, ensure the device meets the minimum security requirements (i.e., screen lock, latest operating system, anti-virus software installed, device encryption, use Google Chrome browser only) as defined in the Woolworths Technology Handbook Policy. If you are unable to meet any of these requirements, use a Woolworths-provided device instead.

❑ Never use removable media (for example USB or SD Card) and mobile devices (SMS, MMS, Instant Message) to store or transfer Woolworths Restricted or Confidential Information, unless for an approved business need and adhering to Cyber Security Standards.

❑ Ensure only standard computer equipment connects to the Woolworths network as defined in the Woolworths Technology Handbook Policy.

❑ Report all incidents or suspected incidents to the IT Service Desk. If you find malicious software on equipment containing Woolworths' information, immediately switch off your device and contact the IT Service Desk on 1800 008 584 (Australia) or 0800 501 801 (New Zealand)

Follow This Policy

Data Classification Standard

This Policy is published in line with the Data Classification Standard and as such applies to the security of Woolworths' information and the information of its customers, for which we each have a trusted responsibility to protect.

Data classification is used to assign a level of sensitivity to information. The classification of information helps to determine the extent to which information should be controlled and secured as it is being accessed, created, amended, stored or transmitted. Information should be handled and protected according to the following 4 classifications:

❑ **Public Information** is information that is already publicly available. For example, press releases and approved advertising brochures.

❑ **Internal Information** is information that is used by Team Members that has not been approved for sharing with the general public. For example, internal company policies, organisation charts and internal communications.

❑ **Confidential Information** is any information protected by company policy or requires authorised access or carries significant commercial risk if released publicly. For example, performance metrics, pricing models or marketing material not as yet authorised for public distribution.

❑ **Restricted Information** is any personal or other information that is protected by law and that requires the highest level of access control and security protection, whether in storage or in transit. For example, credit card information or employee salary.

The misuse or loss of any Confidential or Restricted information may have legal and regulatory implications for Woolworths Group and/or for the individual.

Related Policies

In conjunction with this Policy, ensure you have read, understood and agreed to the Woolworths Code of Conduct, Woolworths Group Cyber Security Policy, Woolworths Technology Handbook and Woolworths Group Data Principles.

Exception

There are some specific IT roles which are authorised to perform duties that would otherwise be in breach of this Policy. These individuals are given express approval to perform these duties within the limits of their role and as such are provided with mandatory privileged access training in line with the Privileged Account Guidelines.

Non-compliance

Non-compliance is an action that is contrary to the statements set out in this Policy.

Non-compliance may result in disciplinary action, including dismissal and/or legal action at Woolworths' sole discretion.

Any suspected breach or non-compliance of this Policy must be promptly reported to the Line Manager, Culture & People Partner, and the Cyber Security Team.

Woolworths may monitor or inspect any material, which is or has been created, sent, received or stored, to ensure compliance with this Policy and prevent inappropriate use.

Woolworths may block Internet sites, applications, add-ons and devices deemed unacceptable, unproductive, or present a risk to Woolworths' information and systems or Team Members.

Policy Changes

This Policy has been reviewed and approved by the **Chief Security Officer** in September 2022. This Policy may be amended or replaced at any time at the absolute discretion of the Chief Security Officer or authorised delegate. It is the responsibility of all Team Members to keep up to date with any Policy changes.