We Always Do The Right Thing

We always do the right thing for our customers, our team members and our brand reputation.

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 and consistently achieve high net promoter scores.

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 and Team Members.

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, support offices, stores, distribution centres, working remotely from home 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 or HR Partner.

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**.

Protect Woolworths' Information

Protect Woolworths' customer, team members and business information from misuse and loss.

It is your responsibility to:

- ❑ **Only collect, use, retain, 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 Information Classification, Protection and Handling section of this Policy).
- ❑ **Never send or store Woolworths Restricted Information such as credit card numbers, unless it is part of an authorised business process or activity that is compliant with Payment Card Industry (PCI) standards.**
- ❑ **Never send or store Woolworths Restricted Information such as PINs, or CVVs by any form.**
- ❑ **Never disclose Restricted or Confidential or Internal Information to unauthorised individuals.**
- ❑ **Physically secure hard copies of Restricted, Confidential and Internal Information when unattended.**
- ❑ **Protect Woolworths' customer information from misuse** (for example, only use customer information for the purpose for which it was collected) **and loss.**
- ❑ **Ensure whiteboards and presentation aids are erased or secured at the end of a meeting.**

Protect Woolworths' customer, team members and business information from misuse and loss.

Use Email and Internet Safely

Report all suspicious emails to hoax@woolworths.com.au

Forward all suspicious emails to hoax@woolworths.com.au for investigation

You must ensure you:

- ❑ **Remain vigilant of suspicious emails 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:**
  - ✔ Conducting non-Woolworths related commercial activities.
  - ✔ Creation or distribution of 'junk' or 'chain' mail.
  - ✔ Subscribe to non-business related services (for example, DropBox, Pokemon Go etc).
- ❑ **Never leak Restricted, Confidential or Internal information between corporate and personal Gmail accounts from any device.**
- ❑ **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.
- ❑ **Never perform any action using Woolworths email and Internet which could bring the Woolworths brand and reputation into disrepute.**
- ❑ **Promote Woolworths in a positive light on social media.**

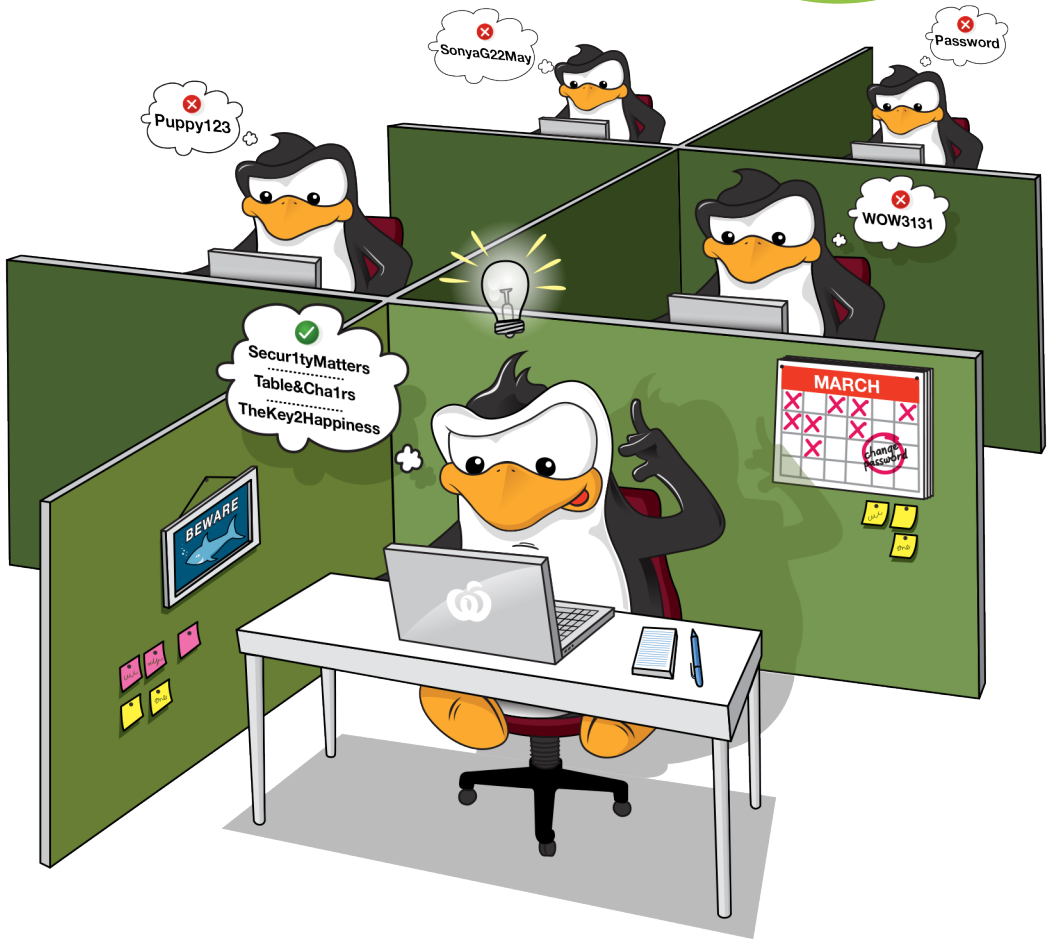
Manage Systems and Information Access

Never share your Woolworths log-on account details or passwords with anyone else. Regularly change the passwords you use to access Woolworths' systems and information.

Implement strong passphrases on all your devices which access Woolworths systems and information.

You must ensure you:

- ❑ **Implement strong passphrases on all devices 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 "10 years ago we visited Japan and had a ball!"** 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)
- ❑ **Do not use the same password for all systems. Use a password manager (for example, LastPass).**
- ❑ **Do not write down your password on paper or electronically save passwords where other Team Members can find them.**
- ❑ **Lock your screen when not in use to prevent other individuals gaining access to the information stored on your device.**
- ❑ **Disable access to systems accounts, when direct reports leave the employment of Woolworths, or a job role changes, which no longer requires the same entitlements.**



Secure Your Devices

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

It is up to you to:

- ❑ Install only approved applications on Woolworths owned devices.
- ❑ Ensure the latest operating system/malicious software detection is installed on your device(s) before connecting to the Woolworths network.
- ❑ All incidents or suspected incidents are to be reported 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.
- ❑ Secure Woolworths' IT equipment at all times (for example, radio frequency guns, store iPads/ tablet devices, laptops, desktops).
- ❑ Never use your device to SMS, MMS or Instant Message features to send Internal, Confidential and/or Restricted Information.
- ❑ Never use removable media (e.g. USB or SD Card) and mobile devices to store Restricted or Confidential Information.
- ❑ Never leave USB keys or mobile devices unattended.
- ❑ Contact the IT Service Desk Team for guidelines about keeping devices safe, prior to travelling overseas on business.
- ❑ Ensure any third party computer equipment is not connected to the Woolworths network.
- ❑ Immediately report any Woolworths' device loss to your Line Manager.

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

Follow This Policy

Information classification, protection and handling

This Policy applies to the security of Woolworths' information and the information of its customers, for which we each have a trusted responsibility for its protection.

Information 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, basic customer information or 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 confidential or personal information that is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. For example, credit card information, income / employee salary or sexual orientation.

The misuse or loss of any sensitive 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** and **myDevice Policy**.

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 via the **Information System Privileged Accounts Policy**.

Non-compliance

Non-compliance is an action that is contrary to the information security principles, policies, standards, guidelines or operational procedures.

Non-compliance of this Policy 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, HR 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 deemed unacceptable, unproductive, or presents a risk to Woolworths' information and systems or Team Members.

Policy Changes

This Policy may be amended or replaced at any time at the absolute discretion of the Director of HR or authorised delegate. It is all Team Members responsibility to keep up to date with any Policy changes.