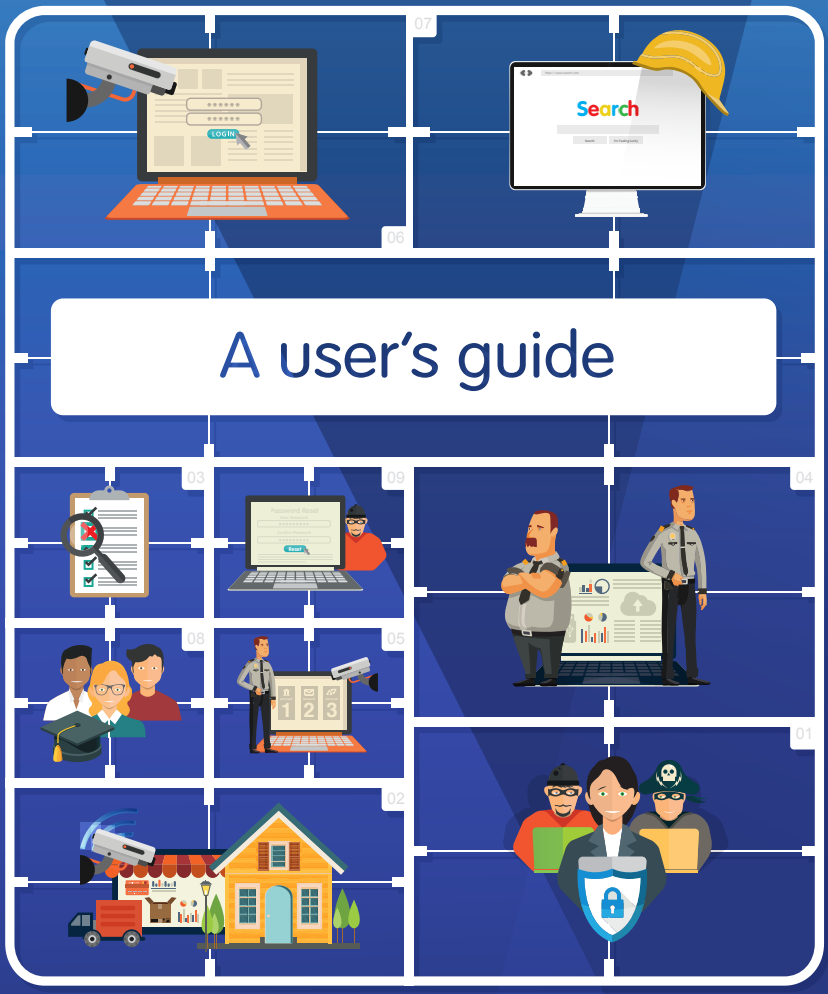
Ensuring your IoT is secure



IoT Alliance Australia

Proudly delivered via the generous funding of Accenture.

Understanding and taking control of your IoT security, safety and privacy.

Foreword

Welcome to the Internet of Things (IoT) user's security guide. This guide provides tips and techniques for you to stay secure and safe when dealing with IoT systems.

For most of us, the internet has opened up new opportunities. We can shop, bank, research, work and connect when and where we want to. Unfortunately, the online world also gives criminals opportunities to steal money, information or identities, so we need to ensure our online environments and devices protect our privacy.

So how do we reduce our risk of falling victim? The Internet of Things Alliance Australia (IoTAA) provides this information and service to help you stay safe when considering devices that connect to the internet at your home and work. Protecting yourself properly means being aware and taking responsibility for your IoT environment and its configuration. This IoT User's Security Awareness Guide assists you, and those around you to stay ahead and stay safe.

This guide has been delivered through the financial support of Accenture. The IoTAA would like to thank them for their generosity.

This IoT User's Security Guide covers eight key areas, and also what you should do if a risk be realised. We hope you will find this guide useful and welcome any feedback you may have.

Matt Tett
Chair
IoTAA WSe3 – Cyber Security & Network Resilience

Security, safety & privacy

Deploying IoT devices is an exciting activity, however protecting IoT users security, safety and privacy becomes increasingly difficult as connected technologies become more prevalent. IoT devices are vulnerable to similar cyber-attacks that affect communications and computer systems. ICT security is reactive, not proactive.

Effective IoT security is critical to safety and privacy

Due to its pervasive nature in our day-to-day lives, vulnerable IoT introduces the additional risk of safety to human lives and wellbeing. IoT security should be incorporated by design, not added to products afterwards, providing stability for delivery of safety and privacy.

Security flaws in most computer systems are patched via updates. IoT devices may not be designed with the ability to easily patch their software, and security vulnerabilities may go unaddressed. Users also forget what IoT products they have connected to their networks and do not maintain their security leaving them open to attack. IoT devices have longer lives than other technologies, introducing a risk that the providers will cease support or go out of business.

The design and maintenance of an IoT deployment must consider how security, safety and privacy are impacted, and develop controls that suit each specific installation.

- Know your IoT ecosystem – Map this regularly using the IoT Reference Framework, this way you are aware of what you have to secure, enabling you to identify risks to safety and privacy.
- Be aware of the balance between IoT security, safety and privacy; each will take on different importance depending on the sector in which the solution is deployed. Mapping identifies sectoral risks, compliance and regulatory requirements.
- Ensuring a correct balance will mean IoT security is optimised and resources are not spent on unnecessary controls.

References: IoT Reference Framework Overview;
https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoT-Reference-Framework-v1.0.pdf

Secure your business & home

Secure your business & home

Internet of Things (IoT) technologies are increasingly central to our home and business lives.

Everything is becoming "smart"

Televisions, refrigerators, vacuum cleaners, baby monitors, toys, security systems, cameras, gaming consoles, doorbells, temperature controls and lights are increasingly connected online.

Connected speakers and virtual assistants help manage home devices, play music and check information such as the weather and sports scores. Smart watches track the steps we take, our heart rates, our messages and our sleep, while smartphones embed themselves into almost every aspect of our lives. We are using our computers like never before – including phones, desktops, laptops and tablets – to conduct work and personal activities.

What steps can you take to keep your business, home and personal IoT systems and devices cyber-secure, safe and private?

- Protect your network, wireless networks and IoT devices with strong passphrases.
- Never use the same passphrase across networks or devices.
- Seek providers who offer multifactor authentication on products and enable it.
- Always change the default administrator usernames and passphrases on new network equipment and IoT devices and accounts.
- With all new network and connected device products, install firmware updates (available from vendor websites).

Further reading:
IoT Security Foundation – Consumer IoT Guidance - https://www.iotsecurityfoundation.org/consumer-iot/

Look for security claims

IoT providers are increasingly aware of the risks to user safety and privacy and are building products with good security by design principles.

Save time and money; buy secure

There have been a number of IoT security good practice frameworks, principles, codes, recommendations and standards published globally. Users should be aware of these and seek to purchase products that comply with them.

What to look for when buying IoT products?

- Buy devices that display the IoT Security Trust Mark certification label.
- Ensure there are no default universal passwords.
- Ensure that software/firmware is kept updated.
- Ensure the provider has a vulnerability disclosure program.
- Ensure your network router has an integrated network firewall function and apply suitable rules to control network traffic.
- Ensure your wireless network router supports multiple SSIDs and set one up specifically for IoT devices, and secure that separately to the one your ICT devices connect to.
- Ensure network and IoT providers products offer automatic updates, and enable those features.

Further reading:

IoT Security Trust Mark Certification & Labelling Scheme - www.iotsecuritytrustmark.com

ENISA Baseline Security Recommendations for IoT:
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

ETSI EN 303 645 v2 Cyber Security for IoT: Baseline Requirements
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

NIST NISTIR 8259 Foundational Cyber Security Activities for IoT Device Manufacturers
https://csrc.nist.gov/publications/detail/nistir/8259/final

Codes of Practice for Consumer IoT Security - UK Government
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/773867/Code_of_Practice_for_Consumer_IoT_Security_October_2018.pdf

Australian Government: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

Protect electronic information

Protect electronic information

IoT data can be created, stored and moved from one to many places. How we transmit and where we store this electronic information can greatly impact our privacy and safety. Much of this data is uploaded via the internet to a variety of cloud-based services.

What steps can you take to secure your IoT data?

- Identify critical information that may pose a risk to privacy and safety. Use encryption methods at all points, to securely collect, transmit and store this data.
- Review any references to security, safety and privacy (including ownership of your generated information) in the terms and conditions of any cloud or other IoT service you consider using to store your data. Top tip: You can also research and monitor media coverage related to these service providers, which may give you insight into security incidents and how they were responded to.
- Public networks may be compromised, and public computers could have spyware software installed to capture all your keystrokes, including login information and card numbers.
- Be aware of fake "phishing" emails. Avoid opening unsolicited files, links, or programs. Opening a compromised file/link could expose your system to spyware that captures your passwords or other information you type.
- Install and update anti-malware software on systems.
- Back up information from devices regularly, keep the backup isolated from the device the data is being backed up from. You may back up to a USB, an external hard drive or a secure cloud service. Keep any backup media encrypted with a strong passphrase and in a physically secure location (i.e. a locked cabinet, in a different geographic location – for example, the home of a trusted friend or family member).

Further reading;
Office of the eSafety Commissioner – How to keep your information secure
https://www.esafety.gov.au/women/connecting-safely/the-cloud

Protecting your IoT accounts

Protecting your IoT accounts

Attackers may try to access your IoT accounts to steal information. Their methods may include using computer programs to automatically 'guess' your passwords; sending fake "phishing" emails that attempt to trick you into supplying your details or clicking links; creating false personas to intercept communications; infiltrating your devices to harvest your information; install software that records keystrokes; monitor other activity; deny access to your information, or launch attacks on other systems.

How can you minimise the risk to your account information online?

- Protect all accounts with strong passphrases (a series of words, numbers and symbols).
- Never use the same passphrase across networks, devices or accounts.
- Use a password manager.
- Seek IoT providers who offer multifactor authentication on accounts and enable it.
- Ensure all smartphones and similar devices (assistants, watches) are locked with PINs.
- Use a Virtual Private Network to connect devices to a work network.
- Closely control who can access networks and devices (limit to staff, family and friends).
- Secure devices when not in use by logging out, ensure each user in your business or home has separate login credentials.
- Ensure anti-malware products are installed and updated on any device or network you use to access online accounts.
- Do not respond to any emails that ask you to provide account usernames, passwords or sensitive information – regardless of who they claim to be from. Using a reliable source (i.e. organisation's website) make an enquiry about the email received.
- Do not access online banking or other accounts while using unsecured wireless networks (including public Wi-Fi hotspots).
- Regularly monitor your account logs for unauthorised or unexplained activity.

Protect your digital identity

Protect your digital identity

All of us have established several digital identities through activities conducted online. Your digital identity may include information about you such as your name, images, location, interests, workplaces, qualifications, usernames, passwords, birthdate and a chronology of searches you've made on the internet. Malicious people or groups can use this information to assume your identity for purposes such as obtaining bank or car loans under false pretences.

How can you minimise the risk to your digital identity?

- Avoid over-sharing personal information on social networking sites.
- Minimise personal information provided to social media or other publicly accessible services and use privacy settings to limit strangers' ability to view or harvest this information.
- Avoid creating images or storing photographs that may cause embarrassment if released into the public domain.
- Regularly check information about yourself online and familiarise yourself with privacy and security measures applied by organisations that keep this information. If these measures do not comply with legislation or an organisation's own policies, ask them to make the necessary changes. Involve regulators or the authorities if they fail to address the issue.

Further reading;
Check if you have an account that has been compromised in a data breach
https://haveibeenpwned.com

Browse safely

The internet is a vast repository of information and interaction – pitfalls await unwary users. Compromised websites may entice users to inadvertently download malicious code. A website can appear legitimate, with seemingly authentic text and branding, yet it may be fake - designed to trick you into providing information for a scammer to access.

How can you browse the internet safely?

- Never leave a device with a child unattended, it may enable others to communicate with them via messages, voice or video. Be aware of the safety risks posed by connected toys and devices that may include microphones, displays and cameras.
- Ensure correct spelling of website names in the address bar; look for the 'https' and padlock symbol in the website address bar.
- Where offered, use multi-factor authentication (that requires you to submit more than one credential for access, i.e. a password and a code sent to your mobile phone)
- Consider the risks of storing information in the autofill functions offered by browsers (which may be vulnerable to being targeted by attackers).
- Be aware that cookies used by website owners may track your activity across the internet; consider using private, or incognito, browsing modes.
- Be careful regarding links to web pages included in unsolicited e-mails, websites and documents. Do not click on any suspicious links. Top tip: If you hover with your cursor over a given link, you can check the web address it's directed to – what may look like a legitimate site that's typed out, the actual hyperlink behind that may be obviously incorrect, or slightly misspelled, aimed to trick you into visiting a fake site.

Further reading:
Office of the eSafety Commissioner – How to browse Safely
https://www.esafety.gov.au/women/connecting-safely/web-browsers

Educate others

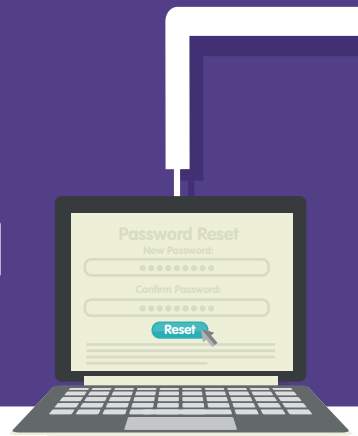
Cyber-security, safety and privacy is not just a personal priority – help protect the people close to you, spread the word. Educate family members, work colleagues and friends. Enable them to identify and avoid visiting suspicious websites, emails and texts. This helps you to protect each other, your business, your connected systems, online accounts, devices and information from malicious software and actors.

How can you educate your family, colleagues and friends about cyber security?

- Avoid spreading fear, uncertainty and doubt. Share cautionary stories about the consequences of failing to adopt secure behaviours that underpin safety and privacy.
- Encourage those in your circles to read this guide and take advantage resources from organisations like the Office of the eSafety Commissioner (https://esafety.gov.au) and the IoT Security Foundation (https://www.iotsecurityfoundation.org)
- Share tips to secure networks, and risks posed using public computers and networks.
- Spread the word that every internet connected device may contain vulnerabilities, ensure they are set to automatically download and apply security updates.
- Advocate unique passphrases for all devices and accounts, remind people to never use the same passphrase, nor share their passphrases with others (even with trusted parties), and always to log out.
- Educate those around you about performing effective backups of their information.
- Assist family to apply good privacy settings to devices, websites or applications.
- Keep social networks of friends secure look for messages that may be suspicious, containing uncharacteristic links or calls to action.
- Let people know that there is no shame in being a victim of cybercrime and it is best to report it rather than hide it; anyone could be a victim at any time. Share details on what to do and who to turn to.
- Recommend installing certified family-friendly filtering software on devices used by children and always monitor the online activities of younger family members. (https://www.commsalliance.com.au/Activities/ispi/fff)

If you have been scammed, hacked or breached

If you have been scammed, hacked or breached



Being scammed, hacked or breached may have serious consequences, however it can happen to anyone. There is no shame in admitting to being a victim. Taking the right steps can help minimise disruption and loss and is far better than trying to hide it.

What steps can I take to recover from being scammed, hacked or breached?

If your online banking or credit card accounts have been accessed by unauthorised parties, inform your bank of any suspicious activity regarding your accounts.
Change your passwords or passphrases and request your account be suspended if you believe you have been breached.

If your home network has been breached:

- Change all passwords, shut the network and connected devices down.
  Seek expert technical help to close the breach and check devices for malware.

If you have been scammed, or suspect a scam:

- Advise your bank and other key service providers.
- Report the activity to authorities and bodies including:
  The Australian Cyber Security Centre ReportCyber service;
  The Australian Competition and Consumer Commission's Scamwatch,
  The iDcare national identity support service.

Further reading;
Australia Cyber Security Centre – What can I report at ReportCyber;
https://www.cyber.gov.au/acsc/report/are-you-a-victim-of-cybercrime
Australia Competition and Consumer Commission – Report a Scam;
https://www.scamwatch.gov.au/report-a-scam
iDcare – National Identity Support;
https://www.idcare.org

IoT Alliance Australia

IoT Security Statistics

$520 billion
the combined IoT market size in 2021. Comprising a lot of valuable data that is attractive to attackers.

26.6 billion
active IoT devices August 2019.
With 127 new IoT devices connecting to the web every second.

98%

of IoT device traffic is unencrypted due to the lack of IoT providers understanding of how to include such security by design.

Reference: https://leftronic.com/internet-of-things-statistics/

IoT Security Awareness Guide
Types of IoT Attacks

Eavesdropping

Unsecure or unencrypted IoT communication channels (e.g. from device to gateways/platform) network can be intercepted and information such as user names, passwords and configuration settings can be captured. Related attacks include man-in-the-middle, session hijacking, or message replay.

Privacy threats / data leakage

Confidential / sensitive data from devices may be captured by hackers during device communications, and disclosed intentionally or unintentionally. This could happen through back door access, and or by MITM attack.

Lack of authentication

IoT devices and system may lack an authentication mechanism and can not verify the authenticity of the SW or FW when updates are being made. An attacker can exploit this vulnerability, and can upload a malicious software package to the device.

Insecure network

Attackers exploit open and insecure network services (Shodan search engine shows HTTP, Telnet, SSH) and turn IoT devices into bots for DDOS attack (e.g., Mirai).

Malware

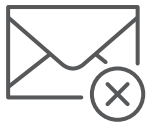
IoT devices can be infected with malware (virus, worm, trojan, etc.) designed to carry out unauthorised actions that could compromise the operation and integrity of the IoT system. The consequence could be data leakage, device hostage, DDOS attack, etc.

Firmware hijacking

Legitimate firmware could be hijacked when the owner of the IoT device tries to download firmware updates, believing the firmware comes from a legitimate source.

Ransomware

It is not unthinkable that ransomware hackers would naturally move on from encrypting files on computers to locking up smart devices, including industrial IoT devices, and demand a ransom to unlock them.



Machine phishing

Hackers could infiltrate IoT devices and command them to send fake signals that will cause the owners to take actions that could damage the operational network.

Trojan horse

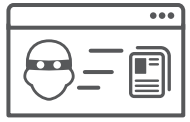
Unsecured IoT devices are Trojan horses themselves. Once infected with malware, they can steal data, spy on people, elevate control functions, perform DDOS attack, and so on.

Cryptojacker

Cryptojacking malware is an emerging online threat that hides on a device and uses the machine's resources to "mine" forms of cryptocurrency, such as bitcoin. Cryptojacking causes high CPU and network usage and drains critical healthcare systems, potentially impacting life-saving capabilities.

Backdoor

Attackers gain access to endpoint devices and/ or system via backdoors such as hardware and software ports, including usb, cellular wireless access, etc. These ports are often used for device configuration and support purposes, but often left unmanaged, or forgotten.



Lack of encryption

An attacker can capture sensitive data if data is transmitted in clear text, i.e., without transport encryption.

Brute-force password attacks

Most (consumer) IoT devices have weak, or guessable default passwords, and brute-force attacks can be effectively used to gain access to the device.

Eavesdropping man-in-the-middle

An eavesdropping or man-in-the-middle attacker might be able to intercept network traffic and steal the sensitive information that IoT devices transmit over the communications channel.

Insecure ecosystem interfaces

Insecure web interfaces leave IoT management systems vulnerable to attacks such as SQL injection, cross-site scripting and cross-site request forgery.

Zombie/Botnet

IoT devices could be hijacked / and turned into botnets in large numbers for conducting DDOS attacks. They can cause chaos and denial of legitimate web servers of their services.

Waterhole / sinkhole

Sinkhole is a type of attack that creates a metaphorical sinkhole in a wireless sensor network node, that compromises the confidentiality of the IoT data and also denies any service to the sensor network. This is done by dropping packets instead of sending them to their destination.

Default settings

Unused SW/HW ports not disabled, and username and password left as default setting.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Notes:

Key IoT security points to remember:

1. Store your critical information in a secure and safe location and back up regularly.
2. Protect your home and business IoT and ICT systems and accounts from cyber-attacks with strong passphrases, strict access controls and robust security software.
3. Review suspicious emails or other electronic messages before responding – including checking with purported senders where necessary – and avoid clicking on links to web pages.
4. Report any compromises or suspicious activity, inform the business, support organisations and government immediately.
5. When it comes to IoT, assist the community to be cyber smart, for their safety and privacy. Educate your family, colleagues and friends to adopt secure online practices, including directing them to appropriate resources for cyber security information.

Ensuring your IoT is secure: A user's guide

IoT Alliance Australia

Disclaimer

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. This information has been prepared by Enex TestLab for the Internet of Things Alliance Australia (IoTAA).

Enex TestLab accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

ISBN: 978-0-9953944-3-8

Ensuring your IoT is secure

A user's guide

IoT Alliance Australia