1. acknowledgement of country

EPA acknowledges Aboriginal people as the first peoples and Traditional custodians of the land and water on which we live, work and depend. We pay respect to Aboriginal Elders past and present. As Victoria's environmental regulator, we pay respect to how Country has been protected and cared for by Aboriginal people over many tens of thousands of years. We recognise the unique spiritual and cultural significance of land, water and all that is in the environment and the continuing connection and aspirations for Country of Aboriginal people and Traditional custodians.

1. Purpose

This policy is an integral component of the EPA Information security framework of policies and standards. EPA provides access to Information assets and IT Facilities to enable its staff to perform their roles and responsibilities. These facilities must be used in accordance with this policy.

1. POLICY PRINCIPLES

The following Acceptable Use Principles (AUP) were applied to this policy's development. These principles can assist in better interpretation of the policy statements.

|  |  |
| --- | --- |
| **Reference**  | **Acceptable use principles (AUP)** |
| AUP-1 | EPA IT facilities are used for performing duties to conduct official EPA business.  |
| AUP-2 | EPA supports work-life balance. Limited and reasonable personal use of IT facilities is acceptable as long as it does not impede the organisation's interests. |
| AUP-3 | EPA is committed to providing and maintaining secure, effective, and reliable IT services to support EPA operations, and all staff have a responsibility to this commitment. |
| AUP-4 | EPA handles Information assets securely in compliance with the Privacy and Data Protection Act (VIC) and external Information owner obligations arising from owner Memorandum of Understanding (MoU) or Contracts. |
| AUP-5 | EPA protects the confidentiality, integrity and availability of Information assets based on their sensitivity level. |
| AUP-6 | EPA employees use organisational resources ethically and lawfully. |

1. policy statements
	1. Handling Information Assets

When handling EPA Information assets, Users must:

1. take reasonable steps to secure any Information assets they create or handle in their capacity as EPA Users. Refer to the [Information Security Policy](https://epavictoria.sharepoint.com.mcas.ms/%3Aw%3A/s/IMPlatformP101/Ecjy8rP5Kd1JgHAVLXzP09EBOhRvthHoUhCnIiB8vlKtdw?e=GG2aYM&McasTsid=20892) and EPA [Protective Information Handling Standard](https://epavictoria.sharepoint.com.mcas.ms/%3Aw%3A/s/IMPlatformP101/ERRYUp_6yQ9PqAOVkE-77B0BTi0q6g40ZhAwAB5aVPURyQ?e=tnAbPt&McasTsid=20892) for specific details, or consult your manager if in doubt.
2. only access Information required to perform their official duties.
3. not access any personal Information or duty holder records unless it is related to a business transaction they are authorised to perform, in accordance with relevant legislation.
4. use their own personalised access credentials and not share them with anyone, including other EPA staff.
5. only disclose Information assets upon explicit authorisation or delegation for designated business purposes and through approved communication channels or IT platforms. e.g., SharePoint portal, Briefings and Correspondence ([BAC](http://sp13intranet/NewsEvents/Pages/EPA%27s-new-Ministerial-Briefings-and-Correspondence-System.aspx)).
6. maintain privacy when accessing Information assets or communicating in public locations (e.g., telephone calls or using a Surface Laptop on public transport). Users should take extra care to minimise the chance of being recorded, overheard, or a device screen being read by unauthorised persons.
7. keep desk surfaces clear of Information contained in hard copy files, documents and other records and unprotected electronic portable storage media.
8. lock computer screens and mobile devices requiring authentication to unlock the screen.
9. physically secure devices that contain Information assets when unattended to avoid theft and unauthorised access.
10. ensure Classified Information stored on local desktops and laptops is securely deleted or moved to a designated system.
11. only use EPA Information security authorised encrypted portable storage media or USB drives.
12. ensure that any documents are removed from printers and fax machines as soon as possible. Classified information must be securely disposed of using shredders or secure bins.
13. ensure that the bulk transfer and exchange of Information assets between the EPA and third-party organisations, partners or vendors are assessed by EPA Information security and recommended security controls are applied.
14. not disclose any EPA Information asset not already in the public domain without explicit authorisation.
15. not make copies of Information assets without explicit approval from asset owners and delete unused duplicates.
16. not send or publish unauthorised comments either on behalf of the EPA or on areas of EPA's interest or area of responsibility for which you are not authorised to comment. Respond to media only as outlined in the [EPA Media Policy](http://sp13intranet/Services/Units/RiskCompliance/corpcompliance/_layouts/15/WopiFrame.aspx?sourcedoc=/Services/Units/RiskCompliance/corpcompliance/Documents/1.%20Policy/Corporate%20Policies/Media%20Policy.pdf&action=default).
17. not wilfully or carelessly transmit confidential corporate Information to an unauthorised recipient.
18. not upload or store Information assets in cloud systems unapproved by EPA IT. This includes online data storage sites, document exchange websites, online multimedia editing and file conversion or personal email accounts.
	1. IT Facilities

EPA IT facilities must:

1. primarily be used for legitimate business purposes and in the interests of serving EPA's function and activities.
2. not be used for commercial gain, advertising, sponsorship, placing a third-party in a position of commercial advantage or result in material loss or liability to EPA.
3. take due care of the physical security of EPA IT devices by protecting items from theft, damage, or unauthorised access at all times.
4. use strong passwords and secure their Multi-Factor Authentication (MFA) tokens to protect their access credentials from being stolen or misused.
5. report any IT equipment loss or theft to the EPA [Service Desk](https://epavictoria.service-now.com/epa/) immediately and assist with any investigations.
6. return all allocated EPA IT Systems and Information assets to the EPA [Service Desk](https://epavictoria.service-now.com/epa/), delegate, or line manager prior to or on the last day of their employment with EPA.
7. use only EPA approved tools and versions for the designated purpose. i.e., Outlook 365 for email, and Microsoft Teams for in-person remote meetings.
8. install and use only copyrighted software for which EPA has an active licence.
9. not share EPA IT devices (i.e., EPA Laptop) with others, e.g., family, or personal acquaintances.
10. not tamper with the security mechanisms built into computing systems, such as disabling security settings or changing configurations.
11. not use proxy anonymisers or public VPN services unless explicitly approved by the EPA Information Security team.
12. not run diagnostics or administrative tools in or against EPA IT facilities. This includes but is not limited to connecting any electronic devices to IT facilities for monitoring data, packets and signals and running Information gathering tools, with the exemption of IT staff required to perform their job.
13. not install or run programs, programming code or devices that could violate any EPA policy or be detrimental to the performance, security, or reliability of EPA IT Systems without prior approval from the EPA Information Security team.
14. not use privileged accounts or system accounts for ordinary business use cases.
15. not download and store sensitive Information on non-EPA computers when accessing EPA business applications. e.g., webmail, teams web, SharePoint. Any copies made must be securely deleted after use.
16. not store, share, transmit, process, display, play or view any illegal, abusive, or offensive material that describes or depicts content in a manner that is likely to offend a reasonable person.
	1. Internet

EPA may block some internet services and websites using filtering technologies without prior notice. Varying levels of access may be provided to Users based on business needs.

Limited private use of the Internet includes the use of Internet banking, weather, news, etc. It does not extend to watching or listening to streaming media for non-work purposes or spending prolonged time on personal browsing.

EPA internet Users must not:

1. download and use unapproved software. Approval requests must be submitted via [EPA Connect](https://epavictoria.service-now.com/it?id=index_it).
2. visit non-business and potentially harmful websites. e.g., games, filesharing.
3. access comments, jokes, images, or any other discriminatory material or material that may be perceived as discriminatory. Refer to EPA's [Preventing and Managing Discrimination, Harassment and Bullying Policy](http://sp13intranet/WorkingAtEPA/Form%20Library/PC-PO-03%20Preventing%20and%20Managing%20Discrimination%20Harrassment%20and%20Bullying%20Policy.pdf) for more information.
4. register with internet forums, personal websites, or social media not related to their EPA job function using a corporate email address.
5. procure or sign-up to new cloud services without explicit approval. Approval requests must be submitted via [EPA Connect](https://epavictoria.service-now.com/it?id=index_it).
	1. Email

EPA may block, delete, or alter email using filtering technologies, frequently adjusted without prior notice.

EPA email Users must:

1. exercise caution when opening emails from an unknown sender or if you’re not expecting them. Be suspicious of messages that aren’t addressed directly to you.
2. verify web links from unknown senders before clicking open; hover over the weblink to see the actual web address; if you do not recognise or trust the address, report this as a suspicious email.
3. report suspicious emails:
* via [EPA Connect](https://epavictoria.service-now.com/it?id=index_it) or calling 96952838
* using provided features within the User platform accordingly, e.g. 'Block sender' and 'Phish alert' in Outlook.
1. take reasonable actions to avoid the receipt of unsolicited emails. These actions could include, not subscribing to unofficial mailing lists, marking unsolicited emails as Junk and adding to Block Senders in Outlook.
2. not use EPA corporate email for sending or receiving emails with abusive or discriminatory comments, jokes, images, or any other material of this nature. Refer to the [Preventing and Managing Discrimination, Harassment and Bullying Policy](http://sp13intranet/WorkingAtEPA/Form%20Library/PC-PO-03%20Preventing%20and%20Managing%20Discrimination%20Harrassment%20and%20Bullying%20Policy.pdf) for more information.
3. not use EPA corporate email to sign-up for personal User accounts in public and commercial forums or websites.
4. not receive or send content that violates any State, Commonwealth, or copyright laws.
	1. Bring your own (BYO) devices
5. EPA allows Users to BYO devices subject to Users agreeing to EPA enrolling their devices for management by EPA Mobile Device Management (MDM) or a similar platform to secure their devices to meet EPA security requirements.
6. Information assets stored in BYO devices must be securely deleted when the device is disposed of, when employment with EPA ends or when the Information is no longer needed.
7. Users must not use any unauthorised or unencrypted BYO portable storage devices such as USB drives, detachable hard drives, or Network Attached Storage (NAS) to store EPA Information assets. Only FIPS-140-2 compliant encrypted devices must be used for business purposes.
8. Wall-mounted network ports on EPA office premises are part of the EPA internal secure network. Users of BYO computing devices such as laptops are not allowed to connect to the EPA internal network. Such personal computing devices are only allowed to use guest Wi-Fi for generic internet access.
9. Users must not connect and use their own network devices (i.e., switches or routers) to extend the EPA network.
	1. Remote Working

When working remotely, Users must:

1. use an EPA approved or configured secure VPN connection, especially if connected to a public Wi-Fi system.
2. use a personal mobile hotspot instead of public Wi-Fi whenever possible.
3. safeguard sensitive and Information assets or documents in your custody.
4. maintain the security hygiene of their home network if used for working from home as per the EPA [best practices for working from home.](https://epavictoria.sharepoint.com/%3Aw%3A/r/sites/grpo365p130/_layouts/15/Doc.aspx?sourcedoc=%7B85CDB2BC-3B3C-4014-B3B3-520CF5D7C31E%7D&file=Information%20Security%20considerations%20when%20working%20remotelyV2.docx&action=default&mobileredirect=true&cid=45b96bc0-421c-426d-9f8f-99629e14cbb6&wdLOR=c857376DA-5FF7-4221-A216-6EBB750F6812)
5. not use shared or insecure computers and accessories to connect to the EPA network remotely.
	1. Intellectual Property

Any intellectual property such as design or architectural documents, process documents, project artefacts, diagrams, analytical reports, or software source code created in EPA while working for EPA belongs to and is copyrighted to EPA.

EPA is potentially liable for misuse of the third-party intellectual property within the EPA environment (e.g., use of unlicensed software). Therefore, EPA Users:

1. must ensure they comply with [intellectual property (IP) rights](https://www.ipaustralia.gov.au/about-us) and contractual obligations relating to the copyright and licensing of all intellectual assets.
2. must adhere to software licence terms and agreements.
3. must not install or use freeware applications without approval. Approval requests must be submitted via [EPA Connect](https://epavictoria.service-now.com/it?id=index_it).
	1. Monitoring

EPA may:

* inspect and disclose the email and web contents using approved technical monitoring, recording, and auditing of EPA Information assets and EPA IT Systems usage as required to comply with legal, technical and policy requirements.
* log User or system activities when this logging is required for operational, maintenance, compliance, auditing, and security purposes.
* monitor/track, filter, intercept, record, read, copy, capture and delete any Information processed as email and/or accessed using the Internet without warning or consent.
* monitoring must be approved by an Executive Director and CTO and can only be performed by authorised personnel under CTOs direction.

This may extend to the following situations:

* Where technical work is required to be undertaken to investigate or resolve an incident,
* Capacity management and planning or the tuning/optimisation of systems resources.
* Where automated systems have been put in place to enforce and / or report on breaches of this policy. e.g., Data Leakage Prevention.
* Where an email has been trapped by the above automation and for the purpose of determining if it should be deleted or forwarded, or for further action, such as reporting.
* Where an investigation is formally undertaken with prior executive management approval, into a staff member's activities.
* Where EPA is required to under law or in relation to enforcing a law.
* EPA may engage managed services providers or other specialist third parties to respond to incidents.
1. application

This policy applies to all EPA and agency staff, EPA service providers and third parties that handle EPA Information assets and/or manage IT systems.

* 1. ****Managing Compliance****

The CTO is accountable overall for ensuring compliance with this policy. The EPA Information Security team is responsible for promoting, monitoring, and managing compliance with the policy across all divisions at EPA.

* 1. ****Non-Compliance****

Non-compliance is an action or inaction that is contrary to the requirements of this policy.

EPA staff are bound by the *Public Administration Act 2004* (PA Act). Section 7(b) of the PA Act requires all public sector employees and other public officials to act honestly in the performance of their duties and to report improper conduct.

This is reinforced by section 3 of the *Code of Conduct for Victorian Public Sector Employees* (the code). The code is binding on EPA staff, and a contravention of it may constitute misconduct. Misconduct, as per section 25 of the VPS Enterprise Agreement 2020, may result in disciplinary outcomes, including termination of employment.

Unlawful activities relating to cybersecurity may be referred to the appropriate law enforcement authorities for criminal/civil proceedings.

Non-compliance with this Policy should be reported to the line manager or the EPA Information Security team via email *itsa@epa.vic.gov.au* or EPA Connect.

* 1. ****Exemptions****

Exemption from the implementation of controls in this policy may be granted through the established procedure. The EPA Information Security team must perform a Security Risk Assessment and recommend options to the CTO for final approval.

1. DEFINITIONS

|  |  |
| --- | --- |
| **Availability** | The desired state that allows authorised EPA User to access defined Information for authorised purposes at the time they need to do so. |
| **Bring Your Own Device. (BYO)** | Using personal devices to connect to EPA networks and access work-related systems and Information assets. Personal devices could include smartphones, computers, tablets, USB drives. |
| **Confidentiality** | The limiting of public sector Information to authorised persons for approved purposes.  |
| **Data/Information** | Data is a collection of individual facts. Information is a collection of data relevant to the recipient at a specific time for a specific purpose. |
| **EPA asset** | Any item (whether tangible or intangible) that has a useful or valuable quality for EPA. This includes Information, physical and personnel assets to support that organisation's business functions, services and activities. i.e., Information, IT Systems. |
| **EPA IT systems** | A discrete set of resources used by EPA; organised for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information. |
| **EPA staff** | All individuals working for EPA, at all levels and grades, including the following, • CEO, Executive Directors, Directors and Managers;• Employees (whether permanent, fixed-term or temporary);• Contractors, consultants, recruitment agency staff and trainees; and• Seconded staff from other Victorian Government organisations.• Students, Interns and Volunteers, paid or unpaid. |
| **Information asset** | A body of Information, defined and practically managed so it can be understood, shared, protected, and used to its full potential. Information assets support business processes and are stored across a variety of media and formats.  |
| **Information Asset Steward** | Is accountable for all information assets for which they are responsible, ensuring each asset is accurate, current, protected, accessible and, if shared, that EPA security and privacy requirements are met. Information Stewards: * Approve rules for the storage, maintenance, retrieval and use of assets allocated to them.
* Ensure that information assets and information systems are classified in accordance with EPA’s Information Classification and Handling requirements.
 |
| **Integrity** | Assurance that public sector Information has been created, amended, or deleted only by the intended authorised means and is correct and valid. |
| **Memorandum of Understanding (MoU)** | An agreement between EPA and third-party outlined in a formal document. It is not legally binding but signals the willingness of the parties to move forward with a contract. |
| **Multi-Factor Authentication (MFA)** | Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN; (ii) something you have (e.g., cryptographic token); or (iii) something you are (e.g., biometric). |
| **PDP Act** | *Privacy and Data Protection Act 2014* (Vic) |
| **Privileged account** | An Information system account with approved authorisations of a privileged User. |
| **Privileged User** | A User that is authorised (and, therefore, trusted) to perform security-relevant functions that ordinary Users are not authorised to perform. |
| **Social engineering** | The methods used to manipulate people into carrying out specific actions, or divulging Information such as Phishing, Watering hole, Pretexting, Baiting, Vishing, Scareware, Honey trap, etc.  |
| **IT Facility** | All of the EPA hardware, software, networks, facilities etc. that are required to develop, test, deliver, monitor, use, control or support applications and IT services. |
| **User** | A person or entity with authorised access to an EPA IT Facilities or Information assets. |
|  |  |

1. REsponsibilities

|  |  |
| --- | --- |
| **Role** | **Responsibility**  |
| **EPA Board** | Approve the Information Security Policies. Support and approve the Information security management and compliance initiatives proposed by the executive. |
| **Risk and Audit Committee (RAC)** | Review and endorse the Information Security Policy. Oversee the effectiveness and performance of EPA information security compliance and risk management. |
| **Chief Executive Officer (CEO)** | Accountable for EPA's compliance with all relevant legislation. |
| **Executive Director Corporate Services**  | The executive sponsor for Information Security management and compliance. Ensure Information security is adequately resourced and prioritised.  |
| **Senior Executive Committee (SEC)** | Accountable to promote Information Security practices and culture and compliance of the Privacy and Data Protection (PDP) Act, by approving policies, training and communication that helps embed Information security in business decisions and processes. |
| **Chief Technology Officer (CTO)** | Responsible to promote Information Security and ensure Information security is incorporated in all organisational programs and projects.  Support and promote the Information Security strategy and road map.Approve/Reject requests for exemptions to parts of this policy to meet specific business needs. |
| **Chief Information Security Officer (CISO)** | Ensures that EPA organisational processes and EPA business operations are conducted to comply with this policy. Responsible for implementation and regular reviews of this policy to ensure it stays current and accurate.Evaluation of exemption requests and providing recommendation.Responsible to monitor, report and manage compliance with this policy across the whole EPA. Responsible to spread awareness of the information security across the organisation through continual communication and training. |
| **Information Security team** | Responsible for developing and promoting the Security framework, associated policies, and supporting documents. Monitor compliance with this policy across the whole of EPA. |
| **All EPA Staff/User** | Comply with the policy statements issued in this policy whenever they handle EPA Information assets and/or manage EPA IT Systems while carrying out the duties and tasks of their EPA role. |

1. FURTHER Information

EPA recognises its legislative and regulatory requirements as a Victorian Government agency and is committed to the principles and practices prescribed by the Public Record Office Victoria as well as those set out in the Information Management Framework for the Victorian Public Service and its associated documents, tools, and procedures.

Statute, case law and regulations govern our business environment and are relevant particularly to the obligation to appropriate handling of Information and not to disclose their contents to third parties without authority.

In using EPA Information, the conduct of all employees is subject to the terms of this policy any other applicable law, policies and/or procedures, including the following:

[Privacy and Data Protection Act (2014)](https://www.legislation.vic.gov.au/in-force/acts/privacy-and-data-protection-act-2014/027) (VIC)

[Equal Opportunity Act 2010](https://www.legislation.vic.gov.au/in-force/acts/equal-opportunity-act-2010/021) (VIC)

[Occupational Health and Safety Act 2004](https://www.legislation.vic.gov.au/in-force/acts/occupational-health-and-safety-act-2004/036) (VIC)

[Information Privacy Act 2000](https://www.legislation.vic.gov.au/as-made/acts/information-privacy-act-2000) (VIC)

[Public Administration Act 2004](https://www.legislation.vic.gov.au/in-force/acts/public-administration-act-2004/079) (VIC) & [Health Records Act (2001)](https://www.legislation.vic.gov.au/in-force/acts/health-records-act-2001/046) (VIC)

[Audit Act (1994)](https://www.legislation.vic.gov.au/in-force/acts/audit-act-1994/067) (VIC) & [Evidence Act (2008)](https://www.legislation.vic.gov.au/in-force/acts/evidence-act-2008/026#rpl-main-content) (VIC)

[Civil Procedure Act (2010)](https://www.legislation.vic.gov.au/in-force/acts/civil-procedure-act-2010/020) (VIC) & [Crimes Act (1958)](https://www.legislation.vic.gov.au/in-force/acts/crimes-act-1958/294) (VIC)

[Victorian Data Sharing Act 2017](https://www.legislation.vic.gov.au/in-force/acts/victorian-data-sharing-act-2017/002) (VIC)

[Code of Conduct for Victorian Public Sector Employees](https://vpsc.vic.gov.au/html-resources/code-of-conduct-for-victorian-public-sector-employees/)

[Disability Discrimination Act 1992](https://www.legislation.gov.au/Details/C2016C00763) & [Sex Discrimination Act 1984](https://www.legislation.gov.au/Details/C2018C00499)

[Spam Act 2003](https://www.legislation.gov.au/Details/C2016C00614) & [Telecommunications Act 1997](https://www.legislation.gov.au/Details/C2021C00237)

[Copyright Act 1968](https://www.legislation.gov.au/Details/C2021C00044) & [Trademarks Act 1995](https://www.legislation.gov.au/Details/C2021C00076)

[Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019](https://www.legislation.gov.au/Details/C2019A00038)

[Freedom of Information Act (1982)](https://www.legislation.gov.au/Details/C2021C00311)

1. approval

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Content authorisation | Date | Quality assurance authorisation |
| Policy Owner | Signature | Chief Technology Officer | Signature |
|  | Samantha Ludolf |  | 30 May 2022 | Abhijit Gupta |  |
| Date | Risk & Audit Committee review | Date | Board approval |
|  18.05.2022 |  |

Date of next scheduled review: May 2024.