

National Integrity Framework

Digital Systems & Information Management

PIPE BANDS AUSTRALIA

Version 1 August 2026

	Name	Position	Date
Prepared by	J Solak	National Management Committee	06-07-2026
Through	National Management Committee		13-07-2026
Approved	National Management Committee		13-07-2026

Version Controls

	Published	Amendments	Responsible Party
Version 1	01-09-2026	Nil, first presentation	J Solak

Contents

Contents	3
Definitions	5
Purpose	5
Relationship to the National Integrity Framework	5
Scope	5
Guiding Principles.....	5
Consistency	6
Security	6
Accountability	6
Continuity	6
Efficiency	6
Information Ownership & Intellectual Property	6
Departure from Office.....	7
Return of Association Information	7
Approved Systems.....	7
Email and Communications Systems	7
Official Email System.....	7
Role-Based Email Addresses	7
Email Provisioning.....	8
Email Forwarding	8
Information Storage and Records Management.....	8
Approved Storage Platforms	8
Recordkeeping	8
Retention and Archiving	8
Official Records and Routine Reporting.....	9
Unauthorised Storage	9
Website and Digital Infrastructure	9
National Website Network	9
Administration	9
Continuity	10
Access Control and Identity Management.....	10
Principle of Least Privilege.....	10
Role-Based Access	10
Changes of Office	10
Identity Verification	10

Cybersecurity Requirements	10
User Responsibilities	10
Password Management	11
Multi-Factor Authentication	11
Security Incidents and Data Breaches	11
Monitoring and Administration	11
Security Controls.....	12
Education and Awareness.....	12
Artificial Intelligence.....	12
Permitted Use	12
Human Oversight	12
Confidential and Sensitive Information	13
Prohibited Use	13
Original Thought and Professional Judgement.....	13
Accountability	13
Exemptions and Special Circumstances	14
Applications for Exemptions	14
Approval of Exemptions.....	14
Conditions	14
Compliance and Breaches	14
Non-Compliance	14
Management of Breaches.....	15
Serious Breaches.....	15
Review and Continuous Improvement.....	15
Appendix A	16
Appendix B.....	17
Email Allocations.....	17
Mail Enabled Security Groups	17

Definitions

Capitalised terms used in this Policy have the meanings assigned to them in the Pipe Bands Australia National Integrity Framework unless otherwise specified.

Purpose

This Standard establishes requirements for the management, security, administration and use of digital systems, information assets and technology platforms used by Pipe Bands Australia.

The objectives of this Standard are to:

- protect Association information and digital assets;
- support secure, consistent and accountable administration;
- ensure continuity of organisational knowledge and records;
- promote effective collaboration and communication;
- support compliance with legal and regulatory obligations; and
- reduce operational, governance and cybersecurity risks.

This Standard complements the National Communications and Online Conduct Policy by establishing operational requirements for digital systems and information management.

Relationship to the National Integrity Framework

This Standard supports the Pipe Bands Australia National Integrity Framework and should be read in conjunction with:

- the Pipe Bands Australia Code of Conduct Policy;
- the Pipe Bands Australia Member Protection Policy;
- the Pipe Bands Australia Safeguarding Children and Young People Policy;
- the Pipe Bands Australia Complaints, Disputes and Discipline Policy;
- the National Communications and Online Conduct Policy; and
- any procedures or guidance documents adopted under the National Integrity Framework.

Scope

This Standard applies to all Relevant Persons and Relevant Organisations who are granted access to Pipe Bands Australia digital systems, information assets, communication platforms or technology services.

This Standard applies regardless of whether access is granted at National, Branch, College, Band, committee or project level.

Pipe Bands Australia operates as a single national organisation. State and Territory Branches form part of the national body and must comply with nationally approved systems, standards and governance requirements.

Guiding Principles

The administration and use of Pipe Bands Australia digital systems must be guided by the following principles:

Consistency

Digital systems should support a unified national approach to communication, collaboration, branding and recordkeeping.

Security

Reasonable steps must be taken to protect information, systems and users from unauthorised access, loss or misuse.

Accountability

Users are responsible for the appropriate use of systems and information to which they are granted access.

Continuity

Association information and records should remain accessible to authorised successors and not be dependent upon individual office holders.

Efficiency

Centralised systems support collaboration, reduce duplication and improve organisational effectiveness.

Information Ownership & Intellectual Property

Information, records, documents, correspondence, publications and other material created, received, stored or maintained in the course of conducting Pipe Bands Australia business remain the property of Pipe Bands Australia, regardless of the device, platform or location used to create, store or access that information.

Unless otherwise agreed in writing by the National Management Committee, any work product created by a Relevant Person in the course of performing an elected, appointed or authorised role on behalf of Pipe Bands Australia is created for the benefit of the Association and forms part of the Association's intellectual property.

This includes, but is not limited to:

- policies, procedures and governance documents;
- manuals, syllabuses and educational resources;
- reports, submissions and strategic documents;
- website content and digital publications;
- correspondence prepared in an official capacity;
- databases, templates and forms;
- photographs, graphics, videos and other media commissioned or created for Association purposes;
- software, source code, automation, workflows and digital solutions developed for Association business; and
- any other material created as part of an official Pipe Bands Australia role.

Relevant Persons act as custodians of these materials while undertaking their role and must take reasonable steps to ensure they remain accessible to Pipe Bands Australia and their authorised successors.

Departure from Office

Return of Association Information

Upon ceasing to hold an elected, appointed or authorised position, a Relevant Person must take reasonable steps to transfer to Pipe Bands Australia, or its authorised representative, any Association records, documents, digital assets, passwords, credentials, source files or other work product created or maintained in connection with that role.

A Relevant Person must not withhold, delete, destroy or claim personal ownership of Association information or work product created in an official capacity.

Approved Systems

Pipe Bands Australia maintains approved systems for communication, collaboration, recordkeeping and administration.

Approved systems may include:

- Microsoft 365;
- Exchange Online;
- G-Suite
- SharePoint;
- Xero;
- Moodle LMS
- Microsoft Teams;
- WordPress;
- TidyHQ;
- Pipe Bands Australia web hosting infrastructure; and
- any other system approved by the National Management Committee.

Association business should be conducted using approved systems wherever practicable.

Association records should not be routinely maintained in personal accounts, privately managed platforms or unauthorised systems where an approved alternative exists.

The National Management Committee may approve additional systems where operational requirements justify their use.

Email and Communications Systems

Official Email System

Pipe Bands Australia maintains a nationally managed email environment for the conduct of Association business.

All official Association business must be conducted using Pipe Bands Australia managed email accounts.

Personal or externally managed email accounts must not be used as the primary means of conducting official Association business unless an exemption has been approved in accordance with this Standard.

Role-Based Email Addresses

Pipe Bands Australia utilises role-based email addresses to support continuity of operations and record retention.

Role-based email addresses remain the property of Pipe Bands Australia and remain active irrespective of changes to office bearers.

Access to role-based accounts may be granted, varied or revoked by authorised administrators.

Email Provisioning

Email accounts are provisioned in accordance with nationally approved structures.

Provisioning arrangements may include:

- individual accounts;
- role-based accounts;
- shared mailboxes;
- distribution groups; and
- mail-enabled security groups.

Email Forwarding

Automatic forwarding of Association email to external accounts may be restricted or disabled to protect organisational information, maintain records and support information security obligations.

Information Storage and Records Management

Approved Storage Platforms

Association documents, records and information assets should be created, stored and shared using approved Pipe Bands Australia systems.

Recordkeeping

Association records must be maintained in a manner that supports:

- continuity of operations;
- accountability;
- transparency;
- historical preservation; and
- compliance with legal obligations.

Retention and Archiving

Pipe Bands Australia maintains records retention and archiving practices to support governance, continuity of operations and compliance with legal obligations.

Unless otherwise required:

- Association records should be retained within approved Pipe Bands Australia systems and infrastructure;
- general administrative records should be retained for a minimum period of seven years;
- governance, historical or archival records may be retained permanently;
- child safeguarding, disciplinary, complaint and other sensitive records may be subject to indefinite or extended retention periods; and
- deletion or disposal of records must be undertaken in accordance with approved procedures and any applicable legal obligations.

Pipe Bands Australia may maintain additional retention schedules or administrative procedures to support the management of specific record categories.

Official Records and Routine Reporting

Pipe Bands Australia maintains a Routine Reporting Policy to support accurate recordkeeping, organisational transparency and effective governance.

Where approved systems exist, Association reports, correspondence and records should be created, submitted and maintained using authorised Pipe Bands Australia systems.

Records maintained through approved systems may be relied upon for governance, audit, operational, historical, complaint and dispute resolution purposes.

Pipe Bands Australia cannot guarantee the availability, completeness or integrity of records maintained solely through personal accounts, private systems or unauthorised platforms.

The use of approved systems supports compliance with the Routine Reporting Policy and assists in ensuring organisational records remain accessible to authorised successors.

Unauthorised Storage

Association records should not be routinely maintained solely within personal devices, personal cloud storage services or private systems where approved alternatives exist.

Website and Digital Infrastructure

Pipe Bands Australia maintains nationally managed digital infrastructure to support communications, administration, membership services and information management.

National Website Network

Pipe Bands Australia maintains a centralised website network, including National and Branch websites.

Branches are expected to utilise nationally approved infrastructure unless otherwise authorised by the National Management Committee.

Administration

Administrative access to websites, hosting environments and related services may only be granted by authorised administrators.

Access must be limited to persons with a legitimate operational requirement.

Continuity

Website content, domains, hosting services and associated digital assets remain the property of Pipe Bands Australia and must be capable of being transferred to successor office bearers without disruption.

Access Control and Identity Management

Principle of Least Privilege

Access to systems and information must be limited to that which is reasonably required to perform an authorised role.

Role-Based Access

Pipe Bands Australia utilises role-based access controls to manage permissions and reduce security risks.

Access rights may be granted, modified or revoked in accordance with operational requirements.

Changes of Office

Where a person vacates an office, role or appointment:

- access should be reviewed promptly;
- access no longer required should be removed;
- organisational information should remain accessible to authorised successors; and
- any Association assets should be returned where applicable.

Identity Verification

Pipe Bands Australia may require reasonable steps to verify the identity of persons requesting access to systems or information.

Cybersecurity Requirements

Pipe Bands Australia is committed to protecting its information, systems and users through the implementation of reasonable security controls and good cybersecurity practices.

User Responsibilities

All users granted access to Pipe Bands Australia systems must:

- take reasonable steps to protect Association information;
- maintain the security of their accounts and credentials;
- comply with security controls established by Pipe Bands Australia;

- report suspected security incidents promptly; and
- cooperate with reasonable security investigations or remediation activities.

Password Management

Users must maintain strong passwords and must not:

- share passwords with other persons;
- reuse compromised passwords;
- deliberately weaken security controls; or
- store passwords in an insecure manner.

Where supported, password management tools should be utilised to assist in maintaining secure credentials.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is mandatory for all Pipe Bands Australia accounts where technically available.

Users must not disable, bypass or otherwise circumvent MFA requirements unless authorised by the National Management Committee or its delegate.

Security Incidents and Data Breaches

Any suspected:

- unauthorised access;
- compromised account;
- data breach;
- phishing attempt;
- malware infection; or
- other cybersecurity incident

must be reported to the National Management Committee or authorised administrator as soon as practicable.

Pipe Bands Australia may take immediate action to protect systems, information or users where a security risk is identified.

Monitoring and Administration

Pipe Bands Australia may utilise reasonable administrative, auditing and monitoring capabilities to:

- maintain system security;
- investigate suspected breaches;
- support operational continuity;
- protect Association information; and
- ensure compliance with this Standard.

Administrative monitoring must be proportionate, reasonable and limited to legitimate organisational purposes.

Security Controls

Pipe Bands Australia may implement security measures including:

- role-based access controls;
- conditional access policies;
- forwarding restrictions;
- audit logging;
- account recovery procedures;
- device management controls; and
- other reasonable security safeguards.

Users must not deliberately circumvent or interfere with security controls implemented by Pipe Bands Australia.

Education and Awareness

Pipe Bands Australia encourages all users to remain aware of contemporary cybersecurity threats and good information security practices.

Education, guidance or training may be provided from time to time to support compliance with this Standard.

Artificial Intelligence

Pipe Bands Australia acknowledges the increasing use of Artificial Intelligence (AI) tools to assist with administration, communications, research, education and content creation.

The Association supports the responsible use of AI where it improves efficiency, productivity or quality, provided such use remains consistent with organisational values, confidentiality obligations and professional standards.

Permitted Use

AI tools may be used to assist with:

- drafting correspondence;
- preparing reports and proposals;
- creating promotional content;
- generating ideas or outlines;
- summarising information;
- educational and training activities; and
- other legitimate Association purposes.

Users remain responsible for reviewing, verifying and approving all AI-assisted content before use or publication.

Human Oversight

Content generated or influenced by AI must not be relied upon without appropriate human review.

Users must exercise professional judgement and take reasonable steps to ensure information is:

- accurate;

- complete;
- appropriate for its intended audience; and
- consistent with Pipe Bands Australia policies and standards.

Confidential and Sensitive Information

Confidential, sensitive or restricted information relating to Pipe Bands Australia, its members, participants, governance activities or operations must not be submitted to public or third-party AI services unless expressly authorised and appropriate safeguards exist.

Users should exercise particular caution when handling:

- personal information;
- complaint and disciplinary matters;
- safeguarding matters;
- financial information;
- legal advice; and
- confidential governance information.

Prohibited Use

AI must not be used to:

- knowingly generate false or misleading information;
- fabricate records, minutes, decisions or approvals;
- impersonate another person without authority;
- misrepresent AI-generated content as independently verified fact; or
- otherwise engage in conduct that breaches Pipe Bands Australia policies or applicable law.

Original Thought and Professional Judgement

Artificial Intelligence should be used as a tool to assist human decision-making, not replace it.

Relevant Persons are expected to contribute their own knowledge, experience, judgement and analysis when preparing communications, reports, submissions, recommendations or other materials on behalf of Pipe Bands Australia.

AI-generated content should be reviewed, refined and adapted by the user to ensure it accurately reflects their views, expertise and intended purpose.

The use of AI to generate content without appropriate human consideration, verification or contribution is discouraged and may be considered inconsistent with the objectives of this Standard.

Accountability

The use of AI does not diminish personal responsibility.

Users remain fully accountable for any content, communication, decision or action created, influenced or supported through the use of AI tools.

Misuse of AI may constitute misconduct and may be managed in accordance with the Pipe Bands Australia National Integrity Framework.

Exemptions and Special Circumstances

Pipe Bands Australia recognises that exceptional circumstances may occasionally prevent full compliance with specific requirements of this Standard.

Applications for Exemptions

A Relevant Person or Relevant Organisation may apply for an exemption where:

- technical limitations exist;
- accessibility requirements apply;
- geographic or connectivity constraints exist;
- operational requirements justify an alternative approach; or
- other exceptional circumstances exist.

Applications should be submitted in writing to the National Management Committee.

Approval of Exemptions

The National Management Committee may grant, refuse, vary or revoke an exemption.

In determining an application, the National Management Committee may consider:

- operational impact;
- security implications;
- organisational risk;
- alternative solutions available; and
- the duration of the requested exemption.

Conditions

Exemptions may be:

- temporary or ongoing;
- subject to review;
- subject to conditions; or
- revoked if circumstances change.

Exemptions will not ordinarily be granted solely on the basis of personal preference where a nationally approved solution is reasonably available.

Compliance and Breaches

Compliance with this Standard is mandatory for all persons granted access to Pipe Bands Australia systems, information assets and technology platforms.

Non-Compliance

Examples of non-compliance may include:

- use of unauthorised systems for Association business;

- unauthorised disclosure of information;
- failure to comply with security requirements;
- unauthorised sharing of credentials;
- interference with security controls;
- misuse of Association systems; or
- failure to comply with lawful directions relating to information management.

Management of Breaches

Where non-compliance is identified, Pipe Bands Australia may take actions including:

- education or guidance;
- corrective action;
- modification or removal of system access;
- administrative action;
- referral under the National Integrity Framework; or
- any other reasonable action necessary to protect Association information or systems.

Serious Breaches

Serious, repeated or deliberate breaches may constitute misconduct and may be managed under the Pipe Bands Australia Complaints, Disputes and Discipline Policy.

Review and Continuous Improvement

Pipe Bands Australia will periodically review this Standard to:

- ensure continued effectiveness;
- address emerging technology risks;
- respond to cybersecurity developments;
- support operational improvements;
- reflect changes to approved systems and platforms; and
- ensure alignment with the National Integrity Framework.

Reviews may be undertaken by the National Management Committee or such other person, committee or working group as determined by National Council.

This Standard may be amended from time to time in accordance with the approval authorities established under the Pipe Bands Australia National Integrity Framework.

Appendix A

Email Provisioning and Role Based Access

Email addresses are provisioned as follows:

National Management Committee & the Australian Pipe Band College

- Receive both a personal address: *Example:* firstname.surname@pipebandsaustralia.com.au
- [and] a portfolio address: *Example:* marketing@pipebandsaustralia.com.au

State/ Territory Branches

- Receive role-based addresses only: *Example:* chair.nsw@pipebandsaustralia.com.au

Where a person vacates a role, the associated role-based email remains active. The new office bearer is granted access, ensuring no communication is lost.

Appendix B

Email Allocations and Role-Based Provisioning

Each state and/ or territory branch is assigned a standard suite of email addresses and mail-enabled security groups. These typically include:

Email Allocations

Chair	chair.state@pipebandsaustralia.com.au
Vice Chair	vicechair.state@pipebandsaustralia.com.au*
Vice Chair 2	vicechair2.state@pipebandsaustralia.com.au*
Secretary	state@pipebandsaustralia.com.au
Treasurer	treasurer.state@pipebandsaustralia.com.au
VP Piping	pipings.state@pipebandsaustralia.com.au
VP Drumming	drumming.state@pipebandsaustralia.com.au
VP Drill & Dress	drill.dress.state@pipebandsaustralia.com.au
VP Rules & Admin	rules.state@pipebandsaustralia.com.au
VP Ensemble	ensemble.state@pipebandsaustralia.com.au

* *Display name may be amended to better indicate associated user.*

Further (optional) addresses may include, yet not be limited to:

Communications	communications.state@pipebandsaustralia.com.au
Scoring	scoring.state@pipebandsaustralia.com.au
Historian	historian.state@pipebandsaustralia.com.au
Education	education.state@pipebandsaustralia.com.au
Councillor	councillor.state@pipebandsaustralia.com.au

Mail Enabled Security Groups

PBX - Branch	branch.state@pipebandsaustralia.com.au	Enabling emails to members of the desired state branch - office holders and college
PBX - College	college.state@pipebandsaustralia.com.au	Enabling emails to the desired state's Vice Principals
PBX – Executive	exec.state@pipebandsaustralia.com.au	Enabling emails to the desired state's branch executive of [state].

Requests for additional or customised addresses must be made in writing to admin@pipebandsaustralia.com.au for review and approval.

**PIPE BANDS
AUSTRALIA**

pipebandsaustralia.com.au