ATENEO DE MANILA UNIVERSITY

UNIVERSITY WEBSITES GOVERNANCE POLICY

DOCUMENT REVISION HISTORY

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
0	Sept. 20, 2023	Data Retention Policy Committee	Initial draft
1.0	Oct. 27, 2023	Data Retention Policy Committee + DITS	Revisions incorporated
1.1	Jan. 26, 2024	Data Retention Policy Committee + DITS	Revisions incorporated
1.2	Feb. 6, 2024	ULCO	Revisions incorporated
1.3	Mar. 18, 2024	Data Retention Policy Committee + DITS	Revisions incorporated
1.4	Apr. 11, 2024	University Library, Data Retention Policy Committee + DITS	Revisions incorporated
1.5	Apr. 28, 2025	Review and Approval by the President's Council	Revisions incorporated
1.6	Dec. 4, 2025	Revisions incorporated and finalized	Revisions incorporated

ATENEO DE MANILA UNIVERSITY

Table of Contents

I. Overview

Websites and online platforms owned and maintained by the Ateneo de Manila University ("University" or "Institution") are vital to its ability to communicate, interact, and share information with communities both inside and outside the University.

As such, they must pass a standard assessment and registration process to ensure their credibility and security and maintain consistency with all applicable standards.

This policy establishes the guidelines for the governance and management of these digital platforms, outlining roles, guaranteeing compliance with cybersecurity and University branding requirements, and promoting a more cohesive and reliable online presence.

II. Scope

This policy shall apply to all University Websites that are affiliated with the University, as well as the offices or units responsible for their development and management, including, where applicable, external suppliers/partners.

It does not cover social media pages and University-managed online systems and platforms such as, but not limited to, AISIS, AIFIS, Edusuite, Canvas, and Google Workspace, which have their own governance, security, and compliance frameworks.

However, any digital presence that uses the Ateneo name and processes personal data in the name of the University shall still follow branding and data protection guidelines.

Meanwhile, websites that are built on the main University website platform (i.e., those with addresses that start with "www.ateneo.edu" and are maintained via cms.ateneo.edu) are deemed automatically registered and approved in accordance with this Policy. Websites built on the main University website have separate registration and development processes but are still governed by general guidelines outlined in this document.

III. Definition of Terms

Affiliated Initiatives	refer to projects, programs, or activities that are linked to a larger organization, institution, or entity, often through some form of partnership, collaboration, or support. These initiatives can take various forms, from research labs and community engagement programs to subsidiary ventures within multinational corporations. They often operate with some degree of autonomy but are still connected to the parent organization, contributing to its overall goals and objectives. Affiliated Labs and Research Initiatives: These are research groups, labs, or units that are associated with a larger institution, such as a university or research center. They may share resources, personnel, or expertise, and their work often aligns with the broader research agenda of the parent organization. Community Engagement: Affiliated initiatives can also involve community engagement programs, where the parent organization partners with local communities to address specific issues or needs. These initiatives may involve research, outreach, or capacity building.
Google Site	A site made with the Google Sites platform, specifically on the Ateneo Google Workspace Platform. These can be open to everyone or just to Ateneo users, and they are often used for internal resources, simple project hubs, or team collaboration. Despite their simplicity, Google Sites are subject to this policy if: ● They carry Ateneo branding

	• They gather or share information about the institution • They are shared with more than one person or a small group
Internal Website	A website intended only for limited audiences, such as specific teams, departments, or classes. These may require Ateneo login credentials and are not indexed publicly. While internal, they must still comply with security and branding standards if they represent a University unit or initiative.
Launch Approval	Formal clearance from UMCO and DITS is required before a website can go live. Approval is granted only after a review of branding, content, hosting, and security.
Personal Data	Pertains to the collective term used to refer to personal information, sensitive personal information, and privileged information.
Personal Information	Refers to any information, on its own or when combined with other information, from which the identity of an individual is apparent or can be reasonably and directly ascertained.
Principle of Least Privilege (PoLP)	A security principle that requires users, systems, or processes to be granted only the minimum level of access—or permissions—necessary to perform their tasks. By limiting privileges to the bare essentials, the risk of unauthorized access, misuse, or accidental damage to systems and data is reduced. Access rights should be regularly reviewed and

	adjusted as roles, responsibilities, or system requirements change.
Sensitive Personal Information	Refers to personal information: (a) about an individual's race, ethnic origin, marital status, age, color, and religious, philosophical, or political affiliations; (b) about an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such individual, the disposal of such proceedings, or the sentence of any court in such proceedings; (c) issued by government agencies peculiar to an individual, which includes, but is not limited to, social security numbers, previous or current health records, licenses or its denials, suspension or revocation, and tax returns; and (d) specifically established by an executive order or an act of Congress to be kept classified.
Site/Service Administrator	The person with technical access to the website's/service's backend, such as the content management system (CMS), hosting dashboard, or Google Site editor. This may be the same as the custodian or someone from IT or a web development team.
Social Media Pages	Official or unofficial online profiles, pages, or accounts on platforms such as Facebook, Instagram, X (formerly Twitter), YouTube, TikTok, LinkedIn, or similar. These channels are used

	to represent, promote, or communicate on behalf of University units, initiatives, or events.
Subdomain	A web address under the primary ateneo.edu domain, structured to represent a specific unit or initiative (e.g., *lawschool.ateneo.edu, archium.ateneo.edu, infosec.ateneo.edu*). Subdomains are only assigned after approval by UMCO (for branding) and DITS (for technical configuration).
Unregistered University Website	A University Website that exists but has **not yet been submitted** to UMCO and DITS for assessment and registration within the prescribed timeframe. ● During the transitory period, existing websites that have not yet undergone registration shall be considered *unregistered*. ● Unregistered websites must immediately undergo the required registration process to avoid being reclassified as unauthorized.
Unauthorized University Website	Unauthorized University Websites are websites that: ● Uses the Ateneo name, branding, or digital credentials (e.g., logo, domain, email address) but was created **outside University-sanctioned processes**, or ● Has **failed to register** within the prescribed deadline and grace period.

	Unauthorized websites are considered non-compliant and may be subjected to takedown, blocking, or other remedial actions by the University. Those that collect or process personal data pose heightened compliance risks and may trigger additional legal or disciplinary measures.
University Website	Any website developed, maintained, or run by an Ateneo de Manila University school, office, unit, department, center, or affiliated initiative. This includes public-facing websites, internal or restricted-access sites, Google Sites, and those built using third-party platforms (e.g., WordPress, Wix) that use Ateneo branding or official email addresses. Some examples are brochure sites or informative pages about the University or any of its schools, offices, units, departments, centers, or affiliated initiatives *[projects, programs, research groups/labs, centers, or activities that are formally recognized by Ateneo through a school, office, unit, department, or center, and that use University identity/resources or operate under University oversight (e.g., covered by a MoA/MoU, University appointment, or funding/support)]*, programs and degrees offered; research endeavors; application, admission, and enrollment processes; faculty, and other information about or related to the institution. Some examples are AUN, AJCU, etc.
University Web-Based Service	An internet-accessible tool or application that provides specific functionality (e.g., registration forms, ticketing tools, surveys, or small-scale web apps) and may be linked from a University Website: • Standalone University-managed systems and platforms (e.g., AISIS, AIFIS, Edusuite, Canvas, Google Workspace) are out of scope for this Policy, as they

	follow their own governance and security frameworks. ● Simple services embedded in or linked to a registered University Website (e.g., Google Forms linked to *www.ateneo.edu*) do not require separate registration but must still comply with University data protection and branding standards. Even if simple or temporary, it is still subject to branding, security, and privacy considerations.
Website Custodian / Point Person	The designated employee or faculty member responsible for coordinating with UMCO and DITS, updating site content, managing access, and ensuring compliance with this policy. The custodian is expected to have: ● Working knowledge of the site's purpose and structure ● Authority to make updates or coordinate with content providers ● Access to the backend or administrative tools of the website

IV. Roles and Responsibilities

Office/Group	Responsibility
UMCO	*University Marketing and Communications Office* ● Supervision and oversight of digital public communications channels, in line with the 31 May 2023 memorandum.

	• Ensure alignment of website development projects with overall University marketing and communications practices and standards • Ensure alignment with University branding, content quality, and visual standards • Provide templates and branding materials as needed
DITS	*Digital Information and Technology Services* • Conduct technical and security reviews • Ensure compliance with institutional cybersecurity standards • Provide hosting support when applicable • Oversee ongoing infrastructure-level and security monitoring, including threats and indicators of compromise (IOCs). • Lead incident response for compromised websites • Maintain the centralized registry of approved websites and subdomains
UDPO	*University Data Protection Office* • Oversee compliance of University Website entries with data protection laws by guiding, reviewing, and monitoring how personal data is collected, used, and safeguarded • Review and monitor the processing of personal data carried out via websites • Where applicable, register websites that process personal data with the National Privacy Commission • Coordinate with DITS and other concerned offices on incidents involving data breaches or violations, and ~~with ULCO~~ on the review of contracts and other related documents
CPO	*Central Purchasing Office* • Ensure vendor/partner accreditation and compliance with University procurement standards
Requesting Unit	• Register the site using the standard form

	• Manage the content which is put into its sites to ensure their accuracy, currency, security and storage • Coordinate with UMCO, DITS, and UDPO as needed • Plan and execute timely decommissioning or archiving for time-bound websites • Assign a Site Administrator and Custodian with appropriate training
Site Administrator	Manage the backend of the website—typically the content management system (CMS), page structure, user permissions, and basic configuration. This role is focused on **content and access administration** and **does not require technical expertise** beyond CMS-level operations. Responsibilities include: • Safeguarding system security (passwords, 2FA) • Managing users or permissions • Coordinating with DITS for hosting and support • Where a website processes personal data, notifying UDPO of any suspected personal data breach or security incident • Ongoing monitoring of content and operational health (e.g., broken links, expired certificates, outdated software/plugins) and coordinating with DITS or external vendors for timely remediation. Site administrators must use official ateneo.edu accounts and enable two-factor authentication. Additional notes on the roles and responsibilities of a site administrator: • If the website is hosted within the Ateneo cloud, infrastructure, security, and technical configuration are handled by DITS. • If hosted externally, technical tasks such as hosting, patching, and backups will be performed by a third-party vendor, but the Site Administrator remains accountable for coordinating with the third-party vendor and ensuring overall compliance.

	• In some cases, the Site Administrator and third-party vendor may be different people, with clearly defined scopes of responsibility. For third-party vendor responsibilities, see Section VIII: Third-Party Vendors.

UMCO & DITS (Joint)	• Jointly review and approve web development projects before they are launched:
	  ○ UMCO for branding and communications compliance.
	  ○ DITS for technical and security compliance.
	• Conduct periodic reviews of active websites for compliance with branding, content, and technical requirements
	• Conduct enablement sessions for new custodians and admins

V. Assessment and Registration

A. General Process

All units that plan to develop and maintain a website that will be affiliated with the University ("Requesting Unit") must formally submit their plans for the same to UMCO and DITS for assessment and registration using the form in Appendix A.

DITS shall thereafter evaluate the plan in terms of technical viability and security while coordinating with other concerned offices, including, but not limited to, the following in the indicated aspects:

- UMCO—for branding and alignment with University communications standards.
- UDPO—for data privacy, including review of privacy notices/consent mechanisms, the possible need for a Privacy Impact Assessment, or registration of additional data processing systems with the NPC.
- ULCO—for legal and regulatory compliance.

DITS shall indicate in writing all its initial observations and recommendations, together with those given by the other concerned office/s. It shall then refer the consolidated initial assessment report to the submitting unit.

Unless the recommendation is to cancel or not proceed with development of a website, the submitting unit may move forward with its plan to develop the planned website while taking into account the observations and recommendations featured in the initial assessment report. If the services of an external supplier/partner are engaged for this purpose, the Requesting Unit shall submit the draft contract to DITS (together with Appendix A), which will coordinate with UMCO, ULCO, UDPO, and other concerned offices as needed for review.

Upon the completion of the configuration of the website, but prior to its launch or deployment, it shall be submitted anew to DITS for its final assessment using the standard Website Registration and Assessment Form (Appendix A). All related documents and relevant information must be attached. DITS shall consolidate the comments, questions, and notes of other concerned offices in the form, including their respective sign-offs, before clearing the website for launch or deployment. No website can launch without the joint clearance issued by DITS (for technical and security compliance) and UMCO (for branding and communications compliance).

Substantial changes to an existing University Website (e.g., major redesigns, significant functional upgrades, or new data collection/processing features) must likewise be submitted to UMCO and DITS for review and clearance prior to implementation. Such changes shall follow the same registration and assessment process as new websites.

Subdomains of ateneo.edu may not be created independently. All subdomain requests must be filed as part of the registration process and require the joint approval of UMCO (for branding) and DITS (for technical configuration) prior to assignment.

Websites intended for research activities must also comply with any applicable research guidelines issued by the University Research Integrity Office (URIO).

B. Technical Standards and Security

To ensure all University-affiliated websites meet institutional cybersecurity, data privacy, and operational resilience requirements, the following technical and security standards must be observed:

1. Secure Communication

- All websites must use HTTPS (TLS 1.2 or higher) to ensure encrypted communication between users and the server.
- Non-secure (HTTP) access must be disabled or automatically redirected to HTTPS.

2. Identity and Access Management

- Websites must be administered using official Ateneo email accounts under Google Workspace to maintain accountability and traceability.
- Two-factor authentication (2FA) must be enabled for all administrative and privileged accounts.
- The principle of least privilege must be enforced to limit access only to those with a legitimate operational need.

3. Hosting and Infrastructure Requirements

- Websites must be hosted on DITS-approved platforms or University-managed infrastructure that supports
    - Regular system and application-level backups
    - Proper access controls, including role-based access
    - Timely patch management and updates
- Third-party or cloud-hosted websites must undergo evaluation to ensure compliance with University hosting and data protection standards.

5. Vulnerability Assessment and Penetration Testing (VAPT)

- Prior to going live, all new University websites or significant changes thereto must undergo
    - A Security Risk Assessment conducted by DITS—Information Security Office

- A Vulnerability Assessment and Penetration Testing (VAPT) conducted by DITS or an authorized third-party service provider, in order to identify and remediate exploitable weaknesses

These evaluation processes shall help identify and resolve, or at least mitigate, critical vulnerabilities before a University website can be publicly launched. Each one shall be documented via a summary of findings and all remediation actions taken.

6. Security Monitoring

- Once live, websites must be monitored regularly for:
  - Security threats or indicators of compromise (IOCs)—by DITS–Information Security Team
  - Broken links, expired certificates, and outdated software components—by the Requesting Unit/Site Administrator, or by the external vendor if hosted outside Ateneo-managed infrastructure.
- Periodic security reviews will be conducted by DITS to ensure continued compliance with University security policies and standards.

C. Requirements for Content and Branding

Websites must adhere to University branding and communications standards, specifically the following:

- Alignment with University public communications guidelines (i.e., Social Media Guide, Public Communications Policy)
- Proper use of University and/or unit/school branding
- Alignment with Branding Guidelines regarding use of fonts and color schemes

When necessary, UMCO will supply standard communications materials such as logos, fonts, and website templates.

Websites should also have the following:

- Link to the University website, www.ateneo.edu

- Link to the relevant University Privacy Notice/s
- Registration Seal issued by the National Privacy Commission
- Contact details of the unit/office managing the website

D. Data Privacy

A website that collects, generates, or processes personal data in any other manner must comply with the Data Privacy Act of 2012 (RA 10173), its Implementing Rules and Regulations, and all other applicable data protection laws and regulations, including those issued by the University.

As a minimum, it shall:

- link to the applicable Privacy Notice of the University, or feature its own dedicated Privacy Notice
- make sure it has a legal basis for its data processing activities. For this purpose, it shall consult with UDPO in order to make a proper determination.

Where an external supplier/partner is involved in the development and maintenance of the website, UDPO may require the execution of a supplementary contract featuring appropriate data protection obligations.

UDPO may also prescribe the conduct of a Privacy Impact Assessment, especially where a website involves high-risk data processing activities or sensitive personal information.

E. Legal and Compliance

The Requesting Unit must ensure that the website's contents do not violate any laws, including intellectual property (IP) laws. The University must own all videos, images, text, marks, and other content displayed on the website, have the proper license to use them, or be within the public domain. Furthermore, the site/service must not contain any video, image, text, or other content that is false, misleading, or harmful to the reputation of the University or another person/entity.

Websites should have Terms of Use or an Acceptable Use Policy clearly outlining the conditions under which users are allowed to use the site, including the standards of conduct required of them.

VI. Non-Compliance and Remedial Actions

To ensure accountability and consistent enforcement of this Policy, University websites may be classified as unregistered or unauthorized, with corresponding remedial actions:

A. Unauthorized University Websites

Definition: University-affiliated websites that (a) are created outside of sanctioned processes or (b) fail to register within the prescribed deadline and grace period.

Remedial Actions:

- May be taken down or blocked by DITS.
- May be removed from official directories and search indices.
- May be flagged to UMCO for branding and communications policy violations.
- May be flagged to UDPO if personal data is collected or processed without authorization, with potential escalation to legal or regulatory remedies.
- Non-compliance may be subject to disciplinary action under applicable University policies.

Non-registration and other instances of non-compliance with this policy may be subjected to appropriate disciplinary action by the University.

Appropriate remediation or updating will be required before sites/services that are taken down or blocked can be reinstated or re-approved for relaunch.

Note on Unregistered Websites (Transitory Period Only):

During the six (6) month transitory period defined in Section IX, existing websites that have not yet been submitted for registration will be considered *unregistered*. Requesting Units will be required to submit such websites within thirty (30) calendar days of notice. After the transitory period, any site that remains unregistered shall automatically be deemed unauthorized.

VII. Website Lifecycle Management

To ensure proper oversight throughout the website's lifecycle, the following guidelines apply:

1. Ongoing Maintenance
    - The Requesting Unit must, post-launch, ensure that the website/service remains functional, secure, and up-to-date.
    - Routine checks for broken links, outdated plug-ins or components, and expired certificates must be conducted by the Site Administrator or coordinating DITS personnel.

2. Decommissioning and Archival
    - Requesting Units must inform DITS, which will in turn notify UMCO and other concerned offices, when websites/services are scheduled to be taken down or archived. Temporary or event-specific websites must include a planned takedown date in the registration form.
    - Decommissioned websites with public records or institutional value must follow archival procedures prescribed by DITS.

VIII. Third-Party Vendors

Third-party vendors (external developers or service providers) may be engaged by University units to build, configure, or support Ateneo-affiliated websites. Their involvement is limited to the scope of their contracts and does not imply content ownership or administrative authority unless they are also designated as the Site Administrators. Drafts of all such contracts must be submitted to DITS which shall facilitate their review and evaluation, including proper coordination with other concerned offices.

All third-party vendors must first be accredited by the Central Purchasing Office (CPO) before they may be engaged.

Responsibilities of third-party vendors should, where pertinent, include:

- Coordinating with UMCO and DITS during design, review, and approval phases
- Developing or configuring the sites/services in line with Ateneo branding, privacy, and security requirements
- Managing technical components such as hosting infrastructure, backups, system patches, and source code—particularly for sites/services hosted outside the Ateneo cloud
- Turning over complete documentation, credentials, and technical access to the unit and/or designated Site Administrator
- Supporting pre-launch testing, technical remediation, and contracted post-launch services
- Ensuring that the site/service platform, plug-ins, and related components remain current and secure, including applying system updates and security patches in a timely manner

Where websites are hosted externally, vendors are responsible for infrastructure-level monitoring, patching, and certificate renewals, while the Site Administrator ensures coordination and compliance.

For sites/services hosted outside Ateneo's infrastructure, third-party vendors are fully responsible for infrastructure-level tasks. The Site Administrator, in such cases, is not accountable for hosting, security patching, or backup management unless these responsibilities are explicitly part of their designated roles.

The Requesting Unit remains responsible for ensuring coordination between the vendor, DITS, and UMCO and for upholding policy compliance throughout the engagement.

IX. Transitory Period

For a period of six (6) months from the issuance of this Policy, all active and/or existing University Websites must be submitted to UMCO and DITS for assessment and registration.

- During this period, such websites will be considered **unregistered** until they are successfully registered.
- After the six-month transitory period, any website that has not been submitted shall automatically be deemed **unauthorized** and subject to the remedial actions outlined in Section VI.

If external suppliers or partners are involved in the management of these websites (in whole or in part), the corresponding contracts and other related documents with these entities must also be submitted for review. This ensures that vendor arrangements are consistent with University requirements on branding, security, and data protection.

DITS shall facilitate the review and evaluation process, coordinating with other concerned offices as appropriate.

A. Monitoring and Policy Review

This policy shall be reviewed **every two years**, or earlier if necessary, to reflect updates in web technologies, cybersecurity practices, and institutional requirements.

In between formal policy reviews, **UMCO and DITS may jointly conduct periodic assessments of selected websites** to verify continued compliance with university branding guidelines, technical standards, and information security and data privacy policies. These assessments may

be conducted on a risk-based or needs-driven basis—for example, during a relaunch, in response to reported issues, or when compliance risks are identified.

Websites found to be non-compliant during such assessments may be subject to the same remedial actions outlined in Section VI, including temporary takedown, delisting from university directories, or required updates prior to continued operation.

X. Contact Information

For policy coordination, assistance, or clarifications, please contact

- University Marketing and Communications Office (UMCO)
  Email: digitalcomms.umco@ateneo.edu

- Digital Information and Technology Services (DITS)
  Email: itsupport@ateneo.edu