Advisory on the Acceptable Use of University IT Resources

1. Introduction

Members of the Ateneo de Manila University community are reminded that their access or use of any or all Information Technology (IT) resources of the University is a privilege granted to them by reason of their affiliation with the University. As such, they are expected to take proper care of such resources and respect the rights of other users, at all times. This includes making sure they are using said properties only for teaching, learning, research, communication, and other related activities sanctioned by the school. Their use must also comply with all applicable laws and regulations, including those relating to intellectual property, cybersecurity, and data protection, as well as contractual and license agreements.

The University issues this Advisory as guidance for the acceptable and effective use of its IT resources.

2. Scope

This Advisory applies to all IT resources owned and managed by the University. It covers all Users of such properties, including University personnel, students, alumni, visitors, affiliates, and service providers.

3. Objectives

This Advisory aims to:

3.1. provide all covered persons with guidance regarding the proper and safe use of University IT resources;

3.2. protect the integrity, reliability, availability, confidentiality, and efficiency of University IT resources; and

3.3. ensure the compliance of the University with applicable laws and issuances related to the use of IT resources.

4. Definition of Terms

Whenever used in this Advisory, the following terms shall have their respective meanings as set forth below:

4.1 "Ateneo Intellectual Property Office" or "AIPO" refers to the unit charged with promoting and implementing the University's Intellectual Property (IP) policy. It provides support to all IP-related activities of the University, including IP generation, protection, and commercialization.

4.2 "Confidential Information" refers to personal data, analyses, computer files, whether or not reduced to written form, compilations, memoranda, notes, reports, studies, data, documents, processes, business strategies, information of all kinds including copies, extracts, and summaries thereof, and all other material containing or based in whole or in part on any such information, disclosed by or stored in the databases of the University via its IT resources.

4.3 “Consent” refers to any freely given, specific, and informed indication of will, whereby an individual agrees to the collection and processing of his or her personal data. There must be a written, electronic, or recorded proof of such consent.

4.4 “Data Breach” refers to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

4.5 “Data Privacy Act” or “DPA” refers to Republic Act No. 10173, which has for its title, “AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES,” as may be amended from time to time.

4.6 “Document” refers to both paper and electronic formats.

4.7 “Encrypted Information” refers to any information that requires a code, key, or password before it can be accessed and used.

4.8 “IT Resources” or “University IT Resources” refers to computers, hardware, software, subscriptions, services, networks, databases, files, electronic files, personal data and other information, software licenses, network bandwidth, username, passwords, documentation, electronic communication, computer laboratories and similar technologies that are owned, managed, or maintained by any office or unit of the University.

4.9 “Information Technology Resource Management Office” or “ITRMO” refers to the unit that provides comprehensive IT services and support to the University community.

4.10 “Intellectual Property Code of the Philippines” or “IP Code” refers to Republic Act No. 8293, which has for its title, “AN ACT PRESCRIBING THE INTELLECTUAL PROPERTY CODE AND ESTABLISHING THE INTELLECTUAL PROPERTY OFFICE, PROVIDING FOR ITS POWERS AND FUNCTIONS, AND FOR OTHER PURPOSES,” as may be amended from time to time.

4.11 “IT personnel” refers to any individual employed or engaged by the University to provide support, implement guidelines, and/or manage the operations of University IT resources.

4.12 “Personal Data” refers to the collective term used for personal information, sensitive personal information, and, to the extent applicable, privileged information.

4.13 “Personal Information” refers to any information, whether 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.

4.14 “Privileged Information” refers to information which, under the Rules of Court and pertinent laws, constitutes privileged communication.

4.15 “Security Incident” refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place. A data breach is a type of security incident

4.16 “Sensitive Personal Information” refers to personal information:

4.14.1 About an individual’s race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;

4.14.2 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 person, the disposal of such proceedings, or the sentence of any court in such proceedings;

4.14.3 Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and

4.14.4 Specifically established by an executive order or an act of Congress to be kept classified.

4.17 "University" refers to Ateneo de Manila University, including all its units, schools, departments, offices, institutes, and centers.

4.18 "University Data Protection Office" or "UDPO" refers to the unit mandated to monitor and ensure the compliance by the University with the DPA, its Implementing Rules and Regulations, and related laws and issuances.

4.19 "University Legal and Compliance Office" or "ULCO" refers to the Unit charged with primarily assisting the University President in overseeing and coordinating legal and regulatory compliance by the school and its units, and in formulating legal strategies for ensuring university sustainability.

4.20 "University Personnel" refers to individuals who perform functions or deliver services for or on behalf of the University, except for service providers. They include, but are not limited to, administrators, faculty members, all types of employees, and consultants.

4.21 "Users" refers to persons who access or operate any IT resource of the University. They include its personnel, students, alumni, visitors, affiliates, and service providers.

5. General Guidelines and Responsibilities

University IT Resources must, at all times, be used in a responsible manner, having due regard for the welfare and best interests of the University and other persons. In line with this, the following guidelines must be observed:

5.1 IT Resources shall only be used in relation to or in support of official activities of the University or any one of its units, or the official functions of its personnel.

5.2 IT Resources shall only be used in a manner that maintains their integrity, reliability, availability, confidentiality, and efficiency.

5.3 Users should, at all times, abide by and respect all applicable laws and policies.

5.4 Users should refrain from seeking unauthorized access to IT resources, or exceeding their authorized permissions.

5.5 Users should adopt necessary and appropriate security measures in relation to their accounts and any IT resource issued to them.

5.6 Users should report any defect, misuse, violation, suspicious activity, or security incident that involves University IT Resources.

5.7 University personnel shall not share or disclose any Confidential Information featured in any University IT Resource.

6. Appropriate Use and Authorization

6.1 *Appropriate Use.* IT resources shall only be used for official or authorized purposes, including those related to teaching, research, communication, administration, and other functions of the University or a specific office thereof. The University reserves the right to decide what shall be deemed appropriate use in specific instances or scenarios.

6.2 *Authorization*. Users may only access IT resources if they have the appropriate authorization, as determined by applicable access restriction policies.

6.3 *Licensed Software.* Users shall only install, access, or operate licensed and/or properly-procured software. Similarly, they may obtain updates or upgrades only from authorized and legitimate sources. When in doubt, they must seek guidance from ITRMO and AIPO.

6.4 *Application and Registration Forms.* Where applicable, Users must accomplish and submit all application or registration forms necessary for the use of University IT resources. They are expected to read, understand, and comply with the terms and conditions set out in these forms.

7. Inappropriate Use

There are different types of inappropriate use of University IT resources. They include the following:

7.1 *Use contrary to law or policies.* IT resources cannot be used for any activity or purpose that is contrary to law or policies, or which encourages any unlawful activity. Examples include:

7.1.1 violation of intellectual property laws, such as the unauthorized copying, reproduction, distribution, removal, alteration, downloading and storage of copyrighted materials

7.1.2 violation of data protection laws, such as the unauthorized processing, malicious disclosure, or improper disposal of personal data

7.1.3 violation of Republic Act No. 10175, or THE CYBERCRIME PREVENTION ACT OF 2012

7.1.4 accessing, viewing, storing, showing, sharing, or exhibiting pornographic materials

7.1.5 unauthorized use of IT resources for personal use/gain of for tasks other than assigned work

7.2 *Use that damages the integrity, reliability, or efficiency of IT Resources.* IT resources cannot be used in a manner that damages or which could potentially damage IT resources. Examples include:

7.2.1 unauthorized system and network activities, such as obtaining configuration information about a network or system over which one does not have administrative responsibility

7.2.2 software or hardware installation or removal, such as the installation, modification, deletion, removal, or destruction of software, databases, operating systems, computer equipment, and network peripherals

7.2.3 disclosure of usernames and passwords that allow other parties to access or operate University IT resources reserved for University personnel or students.

7.2.4 malicious use of IT Resources, such as the intentional introduction of malicious programs to network servers

7.2.5 inappropriate use or sharing of IT resources or privileges, or the use of IT resources for personal gain, commercial use, or other private purposes

7.2.6 engaging in sabotage or intentionally restricting output, or damaging or rendering IT Resources non-operational leading to slowing down of work

8. Privacy and Data Protection

8.1 *Ownership.* University IT resources (including school-issued email accounts and computers) are properties of the University. Thus, the school has the authority to access, inspect, monitor, remove, restrict, and take possession of such resources at any time and for whatever purpose, including when:

8.1.1 determining if an IT resource is being used in accordance with the law and any applicable University policy;
8.1.2 investigating or detecting unauthorized use of IT resources;
8.1.3 monitoring work- or school-related performance; and
8.1.4 facilitating the proper turnover of IT resources between one user to another.

In accordance with applicable statutes and case law, Users shall have no reasonable expectation of privacy when using University IT resources.

8.2 *Processing of Personal Data.* When University IT resources will be used to process personal data, such use must be consistent with the DPA and all applicable laws and policies, including those of the University. When in doubt, a user may consult the UDPO.

8.3 *Confidential and Encrypted Information.* Users shall uphold the confidentiality of any or all Confidential Information they come across when accessing or operating an IT resource. In the case of encrypted information, Users are prohibited from attempting to access the same if they are not the intended recipient thereof or if they are without proper authorization.

9. Enforcement

9.1 *Monitoring*. The University, through the ITRMO, may monitor the use of all IT resources. For this purpose, it may log and check continuously and/or automatically all user activities, and shall take appropriate action if misuse or unauthorized use of IT resources is identified. To prevent abuse of this function, its conduct shall always be done in coordination with ULCO and UDPO. This notwithstanding, all logs shall be deemed confidential and subject to appropriate access restrictions.

9.2 *Reporting*. Users are expected to immediately report to ITRMO or any IT personnel any suspected defect, misuse, abuse, or damage caused upon any IT Resource of the University. Whenever possible, supporting evidence should be included in such report. If there is reason to believe that personal data is also involved, the UDPO shall also be notified.

9.3 *Interim measures.* The ITRMO shall implement either or both of the following interim measures, without need of prior notice to the User, when it deems them necessary to do so to ensure the stability and/or regular operations of the University, or while there is a pending related investigation:

9.3.1 *Deactivation of Use*. ITRMO may deactivate, suspend, or restrict a User's access to IT resources.

9.3.2 *Deletion.* ITRMO may immediately delete, uninstall, or remove any software, hardware, files, or materials that pose a real and imminent threat to the stability or security of IT resources.

9.4 *User cooperation*. Users, as well as other concerned University offices or personnel, are expected to cooperate with the ITRMO and other University offices taking part in any related investigation.

9.5 *Penalties.* Whenever appropriate, the University shall implement disciplinary action against personnel or students who have violated its policies in their actions as users. This is without prejudice to any other relief or remedy available to the school under the law.

10. Disclaimer and Waiver

To the extent allowed by law, the University makes no warranties of any kind with respect to the IT resources it provides. Users are expected to be aware that all IT resources are likely to have inherent defects or deficiencies. As such, they waive any claim for defective or lost work and/or time that may manifest or arise from any such defects or deficiencies. The University cannot be held liable for any resulting damages or losses.

11. Changes to this Advisory

The ITRMO and UDPO may, from time to time, make changes to this Advisory. Such changes will be communicated to all Users either through email or the University website. Any modification will be effective immediately.

Should you have questions or require further guidance regarding this Advisory, you may contact the ITRMO at itrmo@ateneo.edu for IT concerns. If your query involves personal data, data processing, or data protection, you may contact the UDPO at info.udpo@ateneo.edu.

Signed by:

(Sgd) Atty. Jamael A. Jacob
Director
University Data Protection Office

(Sgd) Sandra A. Lovenia
Director
Information Technology Resource
Management Office

Approved by:

(Sgd) Roberto C Yap SJ
President