Policy on Electronic Documents and Signatures
UNIVERSITY OF THE PHILIPPINES SYSTEM

1. Purpose and Scope

1.1. This Policy aims to:

1.1.1. Facilitate the adoption of electronic documents and electronic signatures in transactions with and within the University of the Philippines (referred to as "University") to ensure efficiency while meeting legal and security standards.

1.1.2. Designate secure electronic documents with electronic signatures as the standard for University transactions, in lieu of wet signatures on physical documents.

1.1.3. Establish in University official transactions the minimum requirements for electronic documents and electronic signatures and implement minimum internal rules and controls to ensure document authentication, integrity and non-repudiation of electronic signatures.

1.2. This Policy shall apply to transactions within and with the University such as, but not limited to: electronic communications, procurements, contracts, grant applications, other official documents.

1.3. This policy shall not vary any requirements of existing laws and relevant judicial pronouncements respecting formalities required in the execution of documents for their validity. Hence, when the law requires that a contract be in some form in order that it may be valid or enforceable, or that a contract is proved in a certain way, that requirement is absolute and indispensable.

2. Definitions

For purposes of this Policy, the following terms are defined:

2.1. **Certificate** — an electronic file issued by a certificate authority, used to prove the validity of a public key of a digital signature and serves as evidence of the identity of the signatory of the digital signature.

2.2. **Digital signature** — a secure type of electronic signature bound to an electronic document or electronic data message through public key infrastructure (PKI).

2.3. **Electronic** — carried out, displayed, or accessed by technology whose system of operations is based on the control of small components of an electric current. Methods, devices, and technology that are digital are also electronic.

2.4. **Electronic data message** — information generated, sent, received or stored by electronic, optical or similar means, as defined in RA 8792.

Action of the Board of Regents
at its 1392ND Meeting on 28 AUG 2024
APPROVAL
ROBERTO M.J. LARA
Secretary of the University
and of the Board of Regents

2.5. **Electronic document** — information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically, as defined in RA No. 8792.

2.6. **Electronic signature** — data logically associated with an electronic data message or electronic signature, and attached by the person who intends to authenticate or approve the electronic data message or electronic document. The said data is either

2.6.1. an electronic and distinctive mark or characteristic that represents the identity of the person; or

2.6.2. any methodology or procedure employed or adopted by the person.

2.7. **Private key** — the key used to create a digital signature through encryption.

2.8. **Public key** — the key used to verify, through decryption, a digital signature made with the private key that the public key is paired and associated with.

2.9. **Record** — information or data written or stored in a tangible or electronic medium and can be retrieved and perceived in a human-readable format.

2.10. **Valid** — refers to either —

2.10.1. having legal force; or

2.10.2. in the context of a signature or document in a University transaction, being considered by the University as able to fulfill a requirement for a University transaction to have a signature or document, respectively.

3.Legal Basis

The use of electronic documents and electronic signatures in University transactions is consistent with existing Philippine laws, and their use and operations will be based on government guidelines. The relevant laws and guidelines include:

3.1. Electronic Commerce Act of 2000 or Republic Act No. 8792: "An act providing for the recognition and use of electronic commercial and non-commercial transactions, penalties for unlawful use thereof, and other purposes" dated 14 June 2000;

3.2. Rules on Electronic Evidence (REE) of 2001, or A.M. No. 01-7-01-SC: "Rules regarding electronic data messages being offered or used in evidence" dated 17 July 2001;

3.3. Executive Order No. 810 s. 2009: "Institutionalizing the certification scheme for digital signatures and directing the application of digital signatures in e-government services" dated 15 June 2009; and,

3.4. COA Circular 2021-006: "Guidelines on the use of Electronic Documents, Electronic Signatures, and Digital Signatures in Government Transactions" dated 06 September 2021.

Action of the Board of Regents
at its 1392nd Meeting on 30 AUG 2024
APPROVAL
ROBERTO M.J. LARA
Secretary of the University
and of the Board of Regents

4.Fulfilling Signature Requirements

4.1. When a University policy or legal obligation requires a record to have the signature of an authorized person, an electronic signature bound to the record fulfills this requirement if —

4.1.1. it is considered a valid signature by applicable University policy, including this Policy;

4.1.2. it is legally valid under Philippine law; and,

4.1.3. the signatory of the electronic signature is an authorized person.

4.2. Electronic records are valid in University transactions except when University policy or Philippine law considers them invalid.

4.3. A genuine, authenticated, and integrity-verified electronic signature affixed to a contract, even when made with the consent of the signer and in compliance with this Policy, does not alone ensure that the contracting parties are legally bound to the obligations arising from the contract. A contract cannot be considered legally valid if it does not meet all essential legal requirements.

5.Governance and Procedures

5.1. The University will publish the Manual of Procedures for Electronic Documents and Signatures which will outline the use, validity and operations of electronic documents and electronic signatures.

5.2. The operations and use of electronic documents and signatures in University transactions must comply with the Manual of Procedures for Electronic Documents and Signatures upon its effectivity.

6.Minimum Requirements of Valid Electronic and Digital Signatures

6.1. *Electronic signatures.* An electronic signature must meet all of the following criteria to be considered a valid signature by the University:

6.1.1. A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;

6.1.2. Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all circumstances, including any relevant agreement;

6.1.3. It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and,

6.1.4. The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.

6.2. *Digital signatures.* A digital signature must meet all of the following criteria to be considered a valid signature by the University:

Action of the Board of Regents
at its 1392nd Meeting on 30 AUG 2024
APPROVAL
ROBERTO M.J. LARA
Secretary of the University
and of the Board of Regents

6.2.1. It is considered a valid electronic signature under the criteria outlined in Section 6.1.

6.2.2. Its private key and public key are associated with the signatory.

6.2.3. It is created using its private key and can only be validated by its paired public key.

6.2.4. It is dependent on its private key and the electronic document or electronic data message which the digital signature is bound to.

6.2.5. The electronic document, data message or record that the digital signature is bound to cannot be modified after the latest creation of the digital signature without invalidating the signature.

6.2.6. A vetting process to verify the identity of the owner of the certificate is a prerequisite to the creation of a digital signature.

6.2.7. It was not made with a certificate whose revocation or expiration occurred during or after its creation.

7.*Control processes.*

Control processes and procedures shall be developed in line with the University's Quality Management System (QMS) standards to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records.

8.Training Requirements of Staff

8.1. The University will provide regular training for staff, faculty and students to educate them on the correct procedures for electronic documents and signatures.

8.2. University staff must be trained in the correct use, security requirements, and risks of electronic signatures in University operations, alongside their document routing systems training.

9.Sanctions

9.1. Any individual found violating policies regarding authorized use of electronic signatures, transactions and records shall be subject to disciplinary procedures following existing University standard codes of conduct and applicable laws in the country.

9.2. Any unauthorized and illegal use of electronic documents and signatures shall be penalized under existing laws, rules, and regulations.

10.Effectivity

This policy shall take effect on August 30, 2024.

Action of the Board of Regents
at its 1392ND Meeting on 30 AUG 2024
APPROVAL
ROBERTO M.J. LARA
Secretary of the University
and of the Board of Regents

Selected References

Carminati, B. (2009). Digital Signatures. In L. Liu & M. T. Özsu (Eds.), *Encyclopedia of Database Systems* (pp. 830–835). Springer US. https://doi.org/10.1007/978-0-387-39940-9_131

Commission on Audit (COA) Circular No. 2021-006: Guidelines on the use of Electronic Documents, Electronic Signatures, and Digital Signatures in Government Transactions

Definitions, 15 U.S.C. § 7006 (2022). https://www.govinfo.gov/app/details/USCODE-2022-title15/USCODE-2022-title15-chap96-subchapI-sec7006

Electronic. (n.d.). In *Cambridge English Dictionary*. Retrieved February 16, 2024, from https://dictionary.cambridge.org/us/dictionary/english/electronic

Memorandum No. NGY 22-48: Use of Electronic Documents, Electronic Signatures, and Digital Signatures

Memorandum of Atty. Marlon R. Marquina, Director IV of the COA Systems and Technical Services Sector, Information Technology Audit Office

Republic Act No. 8792: An act providing for the recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes

Rules on Electronic Evidence, A.M. No. 01-7-01-SC (Jan. 7, 2001).

Tennessee Board of Regents. (n.d.). "Use of electronic signatures & records: B-095." https://policies.tbr.edu/guidelines/use-electronic-signatures-records

Action of the Board of Regents
at its 1392nd Meeting on 30 AUG 2024
APPROVAL
ROBERTO M.J. LARA
Secretary of the University
and of the Board of Regents