Frameworks Pictures Internal Data Policy

I. Purpose

Frameworks Pictures needs to protect the security and integrity of its Internal Data without hindering the effective and efficient use of those Data. To achieve this objective, the best efforts of every member of the organization's community is required. The purpose of this Policy is to establish minimum requirements for the appropriate stewardship of Internal Data.

II. Definitions

Internal Data

Internal Data are all of the data and records held by Frameworks Pictures, in any form or medium, for the administration, operation, or governance of the organization or any unit of the organizaion.

Confidential Data

Confidential Data means:

- Internal Data that could, by itself or in combination with other such Data, be used for identity theft or related crimes.
- Internal Data whose public disclosure is restricted by law, contract, organization policy, professional code, or practice within the applicable unit, discipline, or profession.
- Records of the organization's security measures.
- Internal Data whose value would be lost or reduced by unauthorized disclosure or by disclosure in advance of the time prescribed for its authorized public release, or whose unauthorized disclosure would otherwise adversely affect the organization financially.

(Appendix I provides examples of Confidential Data)

Public Data

Public Data are Internal Data that have become generally available to members of the public because a person with authority to do so have intentionally released or distributed them without restriction or limitation.

III. Responsible Use Requirements

Members of the Frameworks Pictures community must comply with the following requirements for responsible use of Internal Data, provided that Sections III(A), III(C)(b), and III(C)(d) do not apply to Public Data.

A. Members of the organization's community may access and use Internal Data only for internal purposes.

a. Members of the organization's community may not use or disclose Internal Data to obtain or provide others with a private benefit that is inconsistent with the organization's interests.

b. Members of the organization's community may alter, store, and distribute Internal Data only for internal purposes.

c. Each member of the organization's community may access Internal Data only if, and then only to the extent that, they need to do so for an internal purpose.

B. Internal Data must be used, stored, transferred, disseminated, and disposed of in ways that minimize the potential for their improper disclosure or misuse.

a. Members of the organization's community must comply with all laws, internal policies, and contracts that govern the use and release of Internal Data, especially Confidential Data.

b. Records that contain Confidential Data and are no longer needed for internal purposes must be disposed of promptly and properly. (Records that contain Confidential Data shall be properly secured to minimize the risk that the Confidential Data will be accessed, either intentionally or inadvertently, by individuals who do not need to see or use the Confidential Data for internal purposes.) Best practices for record disposal are described in Appendix II.

c. Records that contain Confidential Data shall be properly secured to minimize the risk that Confidential Data will be accessed, either intentionally or inadvertently, by individuals who do not need to see or use Confidential Data for internal purposes.

Michigan's Identity Theft Protection Act requires that any records that contain any of the following types of Confidential Data in an unencrypted form be destroyed (shredded or erased) when such Confidential Data is removed from an internal system and the organization is not retaining the Confidential Data elsewhere for another purpose: a person's first name (or first initial) and last name in combination with that person's (a) social security number, (b) driver's license or state personal identification number, or (c) credit or debit card or other financial account number, in combination with any security code, access code, or password that would permit access to that financial account. The Identity Theft Protection Act does not require the destruction of any records needed by the organization for purposes of an investigation, audit, or internal review.

C. Members of the organization's community are individually responsible for the security and integrity of Internal Data in their possession or control, including their proper storage and disposal.

a. Members of the organization's community shall not knowingly create inaccurate or misleading Internal Data or deliberately alter or delete accurate Internal Data to make those Internal Data, or other Internal Data, inaccurate or misleading.
b. Members of the organization's community may share Internal Data only with individuals who need to access those Data for an internal purpose.
c. Members of the organization's community are individually responsible for their own use, storage, dissemination, and disposal of the Internal Data to which they have access.
d. Members of the organization's community who, for internal purposes, make Internal Data available to individuals who are not subject to this Policy should take appropriate action to provide for the proper use, storage, and disposal of those Internal Data by those individuals, including, when necessary, contractual limitations on the further dissemination of the Internal Data by those individuals.

IV. Legally Mandated or Authorized Release

This Policy:

- Does not affect Frameworks' obligations to release data or records when so required by law.
- Does not restrict the authority of appropriate internal officials to determine the time and circumstances for the public release of Internal Data, including Confidential Data.
- Is not intended to discourage the reporting, in good faith, of known or suspected discal or other misconduct or violations of law, regulation, or internal policy to the relevant internal offices or to appropriate external authorities, including, without being limited to, the filing of complaints or grievances under applicable internal policies, procedures, or collective bargaining agreements.

V. Implementation

Unit supervisors/unit administrators are responsible for implementing training and oversight procedures consistent with this Policy for their own units. Links to resources for effective practices for managing confidential data are provided in Appendix III.

VI. Violations

Violations of this Policy may result in disciplinary action, up to and including dismissal of employees. Individuals who violate this Policy may also have their access to certain data sources or software applications revoked. In some cases, they may also be subject to civil and criminal penalties under state or federal laws governing certain Confidential Data.

VII. Additional Resources

Situations may arise for which additional advice may be required. Unit-level data security administrators may be consulted as appropriate.

Updates:

- Original policy published on August 14th, 2025.
- Current policy effective on August 14th, 2025.

Appendix I: Confidential Data

Confidential Data means that data could, by itself or in combination with other such data, be used for identity theft, fraud, or other such crimes.

Examples:

- Social Security numbers
- Payment (credit/debit) card account numbers
- Bank account numbers, automated clearinghouse (ACH), and electronic funds transfer account numbers, brokerage account numbers, and other financial account numbers
- Driver's license numbers and state resident/personal identification numbers
- Passport, visa, and alien registration numbers
- Taxpayer and employer identification numbers
- Employee identification numbers
- Health insurance identification numbers
- Digital keys and passcodes
- Passwords, security codes, access codes, biometric codes, personal identification numbers, and other unique account identifiers
- Personal data such as date of birth and mother's maiden name
- Digital signatures

Confidential data means data and records whose public disclosure is restricted by law, contract, internal policy, professional code, or practice within the applicable unit, discipline, or profession.

Examples:

- Education records (transcripts, enrollment verification, etc.)
- Individually identifiable data in a person's medical record
- Trade secrets or other proprietary business data owned by a third party and provided to the organization upon a promise of confidentiality in a nondisclosure agreement or other contract.
- Proprietary computer applications or source code to which the organization holds a license that restricts further or public distribution
- Bids and proposals until they are opened or the deadline for their review has passed
- Employment data such as retirement account allocations and investments and designation of beneficiaries and personal contacts
- Documentation of grievance, arbitration, and disciplinary proceedings
- Information and records protected by an attorney-client or attorney-work product privilege
- Private financial and other data disclosed under the organization's conflict of interest policies
- Private financial, contact, giving, and other data about donors and prospective donors collected and maintained in connection with the organization's development/advancement activities
- Criminal background check results and other data contained in a consumer report under the Fair Credit Reporting Act
- Data derived from servicing or collecting loans from the organization.

Confidential Data means information about, and records of, the organization's security measures.

Examples:

- Passwords for access to internal facilities or computer systems
- Decryption keys
- Security codes and combinations for locks
- Key codes
- Security plans
- Security procedures
- Threat assessments and preparedness strategies
- Law enforcement deployment plans
- Operational instructions for law enforcement officers and other emergency personnel

Confidential Data means information whose value to the organization would be lost or reduced by disclosure in advance of the time prescribed for its authorized public release, or whose disclosure would otherwise adversely affect the organization financially.

Examples:

- Non-patentable technical information or know-how that enhances the value of a patented invention or that has independent commercial value
- Information relating to the organization's intention to buy, sell, or lease property whose disclosure could increase the cost of that property.
- Finished master video files that have not been released to the public.
- Computer applications to which the organization owns the code.

Appendix II: Best Practices for Record Disposal

Best practices for record disposal are constantly changing as the technologies that contain records evolve.

- NIST Guidelines for Media Sanitization

Paper records should be shredded using a cross-cut shredder, or packaged for confidential shredding by an internal or commercial service in a locked confidential records container made available for this purpose.

Appendix III: Effective Practices for Data Security

Effective Practices for data security are constantly changing as the technologies that contain records evolve. Resources for data security may be found online.