Information Classification and Handling Policy

AUTHORIZED FOR PUBLIC ACCESS AND USE VIA WWW.PROCESSUNITY.COM

Revision History

Revision Date	Summary of Changes	Version	Updated By	Changes marked
3/15/23	Added History and Property sections, Classification, Integrity, Handling policy, Point to InfoSec Handling Matrix		mchatzopoulos	N
5/23/23	Added Masking/Obfuscation specific language		mchatzopoulos	N
8/31/23	Added reference to MS Data disposal processes and NIST-800-88		mchatzopoulos	N
2/11/24	Annual review	2.1	Dstapleton	N
8/30/24	Reviewed for Exchange compliance	2.2	mchatzopoulos	Y
10/29/2024	Updated post privacy update review	2.3	dstapleton	Y
2/4/2025	Annual review and minor edits	2.4	Dstapleton	N
5/22/2025	Re-classified prior to posting to Trust Center	2.5	Dstapleton	N

Document Properties

Status	Check SharePoint for Status
Document Owner	Chief Information Security Officer
Classification	Internal
Approval	CTO
Distribution	All employees

ProcessUnity reviews all policies annually per the Policy Management Policy. Below is an excerpt from the Policy Management Policy regarding policy review, distribution, and acknowledgement.

Annual Review

All policies are reviewed annually by the executive management team for accuracy and required changes. All information security policies must be reviewed by the Vice President of Information Security, Chief Information Security Officer, or the Chief Technology Officer to identify and make any changes required to ensure that the policies remain consistent with business objectives and emerging threats and best practices. Following the annual review, the policies must be re-approved by the Vice President of Information Security, even if no changes are required.

Distribution and Acknowledgement

Applicable policies, along with any associated Standards, Guidelines, Processes, and Procedures, must be made available to all ProcessUnity Workers. ProcessUnity Workers will be informed of any policy changes. ProcessUnity Workers will be required to acknowledge, read, and agree to abide by each Policy as defined by the executive management team:

- Upon hire
- Upon policy change
- Annually

Table of Contents

1. Overview 4
1.1. Purpose 4
2. Scope 4
2.1. Sites and Systems 4
2.2. Operational Responsibility 4
3. Policy Statement 5
3.1. Roles and Responsibilities 5
3.2. Classifications 6
3.3. Privacy and personal data 7
3.4. Handling 9
3.4.1. Confidential and Confidential-Client Copying 9
3.4.2. Public and Internal Copying 9
3.5. Data/Media Disposal 9
3.6. Test Data 10
3.7. Encryption 10
3.8. Retention 10
3.9. Labeling 11
3.9.1. Default Labels 11
3.9.2. Reclassification and Labeling 11
4. Standards 12
5. Enforcement 12

1. Overview

This Information Classification Policy defines the sensitivity of different information and data along with requirements for the use of the classifications and rules for disclosure of classified information.

1.1. Purpose

The purpose of this Information Classification Policy is to ensure:

- ProcessUnity information is properly identified and classified, and handled according to its value, legal requirements, sensitivity, and criticality to the ProcessUnity and its Clients.
- ProcessUnity information receives appropriate and consistent levels of protection to safeguard its Confidentiality, Integrity, and Availability.

It is not anticipated that this technology control can entirely prevent the malicious theft scenario, or that it will detect all data. Its primary objective is user awareness, help mitigate risk of theft, and to avoid accidental loss scenarios. This policy outlines the requirements for data leakage prevention, as defined by numerous compliance standards, industry best practices and associated processes.

2. Scope

2.1. Sites and Systems

This policy applies to all information, including ProcessUnity's information and information shared with ProcessUnity by third parties such as but not limited to clients, partners, and vendors, for which ProcessUnity is the custodian (ProcessUnity Information).

This policy applies to all information in any form including but not limited to databases, electronic documents, printed documents, and verbally communicated information.

This policy applies to any storage device including by not limited to servers, workstations, backup tapes, USB "thumb" drives, loose hard disk drives, floppy disks, file cabinets, and records rooms.

2.2. Operational Responsibility

The Engineering and IT Departments are responsible for ensuring that systems are configured and maintained to meet this policy.

The Office of the CTO, the Product Management Team and the Engineering Department are responsible for ensuring that applications have the features necessary to meet this policy.

All ProcessUnity Workers are responsible for ensuring that their direct handling of ProcessUnity Information of any kind is in compliance with this policy.

3. Policy Statement

All ProcessUnity Workers have a responsibility to protect the Confidentiality, Integrity, and Availability of information collected, processed, transmitted, stored, or transmitted, irrespective of the medium on which the information resides.

- Confidentiality – the expectation that only authorized individuals, processes, and systems will have access to the University's information.
- Integrity – the expectation that the University's information will be protected from intentional, unauthorized, or accidental changes.
- Availability – the expectation that information is accessible by the University when needed.

Information must be classified and handled according to its value, legal requirements, sensitivity, and criticality to the ProcessUnity. Protection levels must be established and implemented relative to the information's classification, ensuring against unauthorized access, modification, disclosure, and destruction. For information governed by law and regulations, the protection levels must satisfy the data security and data privacy requirements.

3.1. Roles and Responsibilities

Data Owner: The person who is ultimately responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management. The data owner shall address the following:

- Review and categorization: Review and categorize data and information collected by his or her department or division.
- Assignment of data classification labels: Assign data classification labels based on the data's potential impact level.
- Data compilation: Ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data.
- Data classification coordination: Ensure that data shared between departments is consistently classified and protected.
- Data classification compliance (in conjunction with data custodians): Ensure that information with high and moderate impact level is secured in accordance with federal or state regulations and guidelines.
- Data access (in conjunction with data custodians): Develop data access guidelines for each data classification label.

Data Custodians/Stewards: are responsible for maintaining and backing up the systems, databases and servers that store the organization's data. In addition, this role is responsible for the technical deployment of all of the rules set forth by data owners and for ensuring that the rules applied within systems are working. Some specific data custodian responsibilities include:

IT Operations:

- Access control: Ensure that proper access controls are implemented, monitored and audited in accordance with the data classification labels assigned by the data owner.

- Data backups: Perform regular backups of state data.
- Data restoration: Restore data from backup media.
- Compliance: Fulfill the data requirements specified in the organization's security policies, standards and guidelines pertaining to information security and data protection.
- Secure storage: Encrypt sensitive data at rest while in storage; audit Storage Accounts administrator activity and review access logs regularly.

Information Security Office

- Audits: Annually, audit the data in scope of this policy with the Data Owners that addresses availability, integrity, and confidentiality of classified data.
- Monitor activity: Monitor and record data activity, including information on who accessed what data.
- Data classification compliance (in conjunction with data owners): Ensure that information with high and moderate impact level is secured in accordance with federal or state regulations and guidelines.
- Data access (in conjunction with data owners): Develop data access guidelines for each data classification label.
- Compliance: Fulfill the data requirements specified in the organization's security policies, standards and guidelines pertaining to information security and data protection.

Data user: Person, organization or entity that interacts with, accesses, uses or updates data for the purpose of performing a task authorized by the data owner. Data users must use data in a manner consistent with the purpose intended and comply with this policy and all policies applicable to data use.

For clarity, all Client Information is the direct property of its respective Client. For the purpose of ProcessUnity policy, the Information Owner of Client Information in ProcessUnity's custody is the ProcessUnity worker with fiduciary responsibility to that Client. This definition of Information Owner does not establish or attempt to establish legal ownership of Client Information by ProcessUnity. Rather, it assigns responsibility for ProcessUnity's operational responsibilities relevant to proper custodianship of Client Information.

3.2. Classifications

The following table defines the classifications for ProcessUnity Information:

Confidential – CLIENT: Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Examples:

- Customer Data: personal information, social security numbers, credit card numbers
- Customer Data: Financial information, supplier lists, mailing lists, encryption keys, and any customer/subscriber data that is considered confidential from a customer perspective.

This classification is also inclusive of any client data that is considered Confidential, as defined below, but is only used when personal, identifying data is present.

Confidential: Information which unauthorized disclosure, compromise, or destruction

could result in severe damage, provide significant advantage to a competitor, or incur serious financial impact to ProcessUnity or its employees.

It is also information that ProcessUnity and employees have a legal, regulatory, and contractual obligation to protect. It is intended for use solely within defined groups within the organization. Unauthorized disclosure, compromises, or destruction would adversely impact ProcessUnity, clients, client contractors, or employees. It is intended solely for use within ProcessUnity and is limited to those with an explicit, predetermined "need to know" basis. The following depict examples of information that would be classified as confidential:

- Internal ProcessUnity Data: Information about new products and services, trade secrets, merger negotiations, patents, proprietary information, new pricing structures, encryption keys, code, and any other information that provides a competitive advantage to ProcessUnity.
- ProcessUnity Data: Personnel records, medical, health and benefit information, payroll information, online access codes, personal information, social security numbers, credit card numbers, financial information

Internal: Information which, due to a technical or business sensitivity, requires special precautions to ensure the integrity of data by protecting it from unauthorized access, modification, or deletion. This information is intended for use only within ProcessUnity and must be limited to employees, agents, and contractors of ProcessUnity.

Examples: Profit earnings forecast, company policies, employee handbooks, contact directories, organizational charts and internal announcements, product road maps.

Public: Information which is or has been made available for public distribution, use and/or general access in an authorized manner. Public information does not require special protection. It is information that can be disclosed to anyone without violating an individual's right of privacy or duty of confidentiality. Knowledge of this information does not, directly, or indirectly, expose ProcessUnity to financial loss, embarrassment, or jeopardize the security of assets.

Examples: Marketing brochures, publicly available annual reports, and press releases.

3.3. Privacy and personal data

Information which contains personal data about an individual (which includes not just contact information, but also any other information which either on its own or together with other information that we hold, identifies an individual, such as IP address) must be handled in accordance with our privacy and data protection obligations.

ProcessUnity must comply with its legal obligations under privacy and data protection laws and regulations in each jurisdiction in which it collect, uses, stores or otherwise handles personal data. Some of those laws are set out in the table below.

You must ensure that whenever you handle personal data, you comply with the following ProcessUnity policies:

- ProcessUnity Corporate Data Protection Policy

- ProcessUnity International Data Transfer Policy
- ProcessUnity Personal Data Consent Policy
- ProcessUnity Personal Data Retention Policy

ProcessUnity maintains the privacy@processunity.com email address. Messages sent to this address are routed to the Data Protection Officer (DPO), where they are re-routed to the appropriate department head or customer support, who will reach out and work directly with the submitter and facilitate communications with the customer as required.

Regulation /Standard	Label	Definition
GLBA	NPI or NPPI	Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
Section 501(b) of the Gramm-Leach-Bliley Act of 1999.	"Non-Public Personal Information"	
HIPAA / HITECH Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009.	PHI "Protected Health Information"	HIPAA Home | HHS.gov
	PHI Identifiers	HIPAA Home | HHS.gov
Mass Privacy M.G.L. 93 H, 93 I and 201 CMR 17.00	PI "Personal Information"	201 CMR 17.00: Standards for the Protection of Personal Information of MA Residents | Mass.gov
General Data Protection Regulation (GDPR)	"Personal Data"	General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu)
UK Data Protection Act 2018 and UK GDPR	"Personal Data"	UK Data Protection Act 2018

In all cases, the basic Classification for this Privacy Information must be one of the following:

- Confidential
- Confidential-CLIENT

3.4. Handling

All information must be adequately handled in accord with the ProcessUnity Data Classification and Handling Matrix.xlsx

3.4.1. Confidential and Confidential-Client Copying

3.4.1.1. Prohibition of Copying

ProcessUnity Workers are prohibited from copying Confidential and Confidential-Client, as defined by the ProcessUnity Data Classification and Handling Matrix.xlsx, from their primary production data-stores. Specifically, ProcessUnity Workers are prohibited from copying any client data from any system located on the Production Network to any other system; including other systems on the Production Network. The purpose of this restriction is to minimize the number of copies of client data to only those copies needed for business operations. The solution architecture already accounts for backups and business continuity; additional copies for this purpose are not permitted.

3.4.1.2. Authorization of Copying

From time-to-time it may be necessary for an administrator to administratively make a copy of Client data. When such actions are required, this activity must be documented as a Change Management ticket and approved by management according to the Change Management Policy.

3.4.2. Public and Internal Copying

Public and Internal Data may be copied by ProcessUnity Workers without prior management approval. ProcessUnity Workers are required to minimize this copying to only that which is required for effective business operations and to destroy any copies that are no longer required.

3.4.3. Data Obfuscation/Masking

The process of modifying sensitive data in such a way that it is of no or little value to unauthorized intruders while still being usable by software or authorized personnel must be used when transferring client data from production or production like systems to test systems (see section 3.6 below) or if a Client wishes to implement this solution inside of their Instance where the controls are available.

3.5. Data/Media Disposal

The information contained within ProcessUnity system hardware which is released from

use must be rendered unrecoverable. Use of the delete or format command is not considered sufficient for removal. It must be destroyed onsite or removed and stored in a secure location clearly marked for hard drive disposal.

Electronic information storage devices (hard drives, tapes, diskettes, compact disks, etc.) and Data stored in Azure must be disposed of in a manner corresponding to the classification of the stored information as set forth below in the ProcessUnity Data Classification and Handling Matrix.xlsx.

Devices or media containing Confidential-Client or Confidential information must be physically destroyed or cleansed using DOD-compliant procedures for data destruction as specified by the Information Security Office.

Any third party used for external disposal of ProcessUnity's obsolete equipment and material must be able to demonstrate compliance with the ProcessUnity Information Security Policies and auditable logs for the destruction of devices and media. Secure disposal shall be evidenced by appropriate Certificates of Destruction issued by the recycler.

Data that is stored in MS Azure and AWS is destroyed based on NIST SP-800-88 Guidelines

Data-bearing device destruction - Microsoft Service Assurance | Microsoft Learn

3.6. Test Data

ProcessUnity Confidential Information or Confidential-Client Information or any Client data stored in the production environment may not be used as test data in any way. It must not be copied to the Development Environment, the Quality Assurance Environment, or any lab environment of any kind.

If new test data based on production data is required, the production data must be stripped of all information that could be used to identify the Customer. All such processing must be done without violating any ProcessUnity policies. (For example, copying Client Information out of the Production Operations environment for the purpose of sanitizing it for the Quality Assurance department is not allowed.)

ProcessUnity employees must work with the Chief Information Security Officer to develop an appropriate strategy for any Client Information sanitization effort.

3.7. Encryption

All copies of ProcessUnity Information that must be encrypted based on the ProcessUnity Data Classification and Handling Matrix.xlsx, must follow the ProcessUnity Encryption Policy.

3.8. Retention

The goals of these data retention rules are two-fold. First, data must be retained in accordance with contractual and regulatory requirements. Second, ProcessUnity must minimize the quantity of Confidential and Confidential Client data it stores thereby reducing the impact of any security compromise.

ProcessUnity Workers must minimize the number of copies of ProcessUnity Information stored. ProcessUnity Information should be retained only in their primary datastores.

Information shall only be retained for the duration required for business or legal purposes.

3.9. Labeling

All ProcessUnity Information must be labeled with its Information Classification. Acceptable methods of labeling include:

- The inclusion of the Classification label on the information itself. For cloud resources Tags are an acceptable form of labelling
- Labeling within a ProcessUnity Policy.
- Removable media must be labeled with the highest information classification that applies to any data on that media. It is the responsibility of the Information Owner[1] to correctly label the ProcessUnity Information they are responsible for.

3.9.1. Default Labels

All ProcessUnity Information not otherwise marked with an Information Classification shall be handled according to the following, default Classification labels.

Information Asset	Default Label
Production Operations Host	Confidential - CLIENT
Production Backups	Confidential - CLIENT
Production IT Host	Confidential
Printed Document	Confidential or Confidential - CLIENT (if Client or Customer information is present)

3.9.2. Reclassification and Labeling

Information owners are responsible for ensuring that if the sensitivity of the data they are responsible for increases, the classification of that data and its labeling is updated in a timely fashion so that it follows this policy. If the sensitivity of data decreases, information owners may update the classification of the data so that it is in compliance with this policy. It shall not be considered a violation of this policy to over-classify data. However, information owners are encouraged to correctly classify their data for efficiency of operations.

The Chief Information Security Officer may correct any misclassification of data.

4. Standards

Please see the ProcessUnity Data Classification and Handling Matrix.xlsx for details

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.