Data Classification and Handling Policy

As part of our mission to provide tuition and debt-free technology courses to low-income students, our organization handles significant amounts of sensitive data. This includes donor information, student personal details, and online payment information. The trust of our students, donors, and partners is paramount, and it is incumbent upon us to protect their data meticulously.

The Data Classification and Handling Policy is our guiding framework to ensure this protection. It establishes clear guidelines for handling, storing, and transmitting different types of data. The policy is not solely about security, but also about demonstrating respect for the privacy of individuals and compliance with applicable laws and regulations.

Understanding and adhering to this policy is a responsibility we all share, irrespective of our roles within the organization. We're committed to helping you understand these guidelines, offering training and support as needed. By adhering to this policy, we uphold our commitment to our students, donors, and the wider community, fostering a secure and trustworthy environment for all.

What is data?

Data is any piece of information that our organization collects, stores, and uses. This can range from simple details like course descriptions to more sensitive information such as donor bank details. Our organization classifies data into four main categories: Public, Internal, Confidential, and Sensitive.

Public Data is information that can be freely shared, within and outside the organization, without any encryption. This might include our course descriptions, public event details, and research publications.

Internal Data should be shared only on a need-to-know basis, even within the organization. It requires basic security measures like password protection for storage and should ideally be sent via secure, authenticated channels. This data typically includes administrative details, internal communications, and operational schedules.

Confidential Data can only be accessed by authorized individuals and is shared strictly on a need-to-know basis. It requires strong security measures, such as encryption for storage and transmission through secure, authenticated, and encrypted channels. Examples of this type of data would be the personal details of students and donors, and proprietary research data.

Finally, Sensitive Data should only be accessed by specifically authorized personnel and is never shared unless required by law enforcement. This type of data must be stored in encrypted form and transmitted only over secure, authenticated, and encrypted channels. The most protected category, sensitive data includes information such as credit card numbers, bank details, and Social Security Numbers of students and donors. By categorizing our data and

handling it appropriately, we can ensure the privacy and security of all the individuals associated with our organization.

Public Data Handling Policy and Procedure

1. Handling:

Public data, including course descriptions, public event details, and research publications, is intended for public consumption. This data can be freely shared, both within and outside the organization. However, while this data is considered public, the integrity and accuracy of the information are crucial. Therefore, only designated personnel should have the authority to create, modify, or delete this information to ensure its accuracy and reliability.

2. Storage:

Public data should be stored on our organization's servers or approved cloud storage providers. Although encryption isn't required for public data, the data should still be protected from unauthorized alteration or deletion. This can be achieved by using appropriate access controls to limit who can modify or delete the data.

3. Transmission:

Public data can be sent over the public internet without encryption. However, secure channels should be used where available, especially when transmitting large amounts of data or updating critical public information.

4. Retention and Disposal:

Public data should be retained as per the organization's data retention schedule. Generally, public data like course details and research publications should be archived when no longer in active use, rather than being permanently deleted. In line with the Payment Card Industry Data Security Standard (PCI DSS), any public data that contains references to payment or donation amounts should be retained for a minimum of one year but should not include any sensitive payment card data.

After the retention period, the data should be archived in a secure environment for another year. Post this period, if there are no legal, regulatory, or business reasons for further retention, the data can be safely deleted.

***Note: This policy does not override any different retention periods specified by other applicable laws or standards, which would take precedence.**

Public data is information that can be freely shared, both within and outside of the organization. Examples of public data include course descriptions, public event details, and research publications. Even though public data does not contain sensitive or confidential information, it should still be handled responsibly to maintain data integrity and ensure its proper usage.

Policy:

1. Usage: Public data should be used for the purpose it is intended for, which is to inform the public about our programs, events, and research findings.
2. Sharing: Public data can be freely shared with any interested party without restrictions, as long as the data's integrity and accuracy are maintained.
3. Security: Although public data does not contain sensitive information, measures should still be taken to protect against unauthorized alteration or deletion.

Procedure:

1. Accuracy: Before public data is shared or published, it should be reviewed for accuracy and relevance. This review should be conducted by the appropriate personnel or department to ensure the data is current and correctly represents the organization's information.
2. Distribution: Public data can be distributed through various channels such as the organization's website, social media platforms, press releases, and public reports. Before distribution, the appropriate department must approve the data.
3. Updates: Public data should be reviewed and updated regularly to ensure it remains current and relevant. Any changes or updates should be communicated as quickly as possible to all relevant parties.
4. Security: While public data is freely shared, it is important to prevent unauthorized modification. Data storage systems should have mechanisms in place to prevent unauthorized users from modifying or deleting the data.

Remember, even though public data does not contain sensitive information, it is still essential to handle it responsibly to maintain trust and transparency with the public we serve.

Internal Data Handling Policy and Procedure

1. Handling:

Internal data includes information such as administrative details, internal communications, and operational schedules. This data is intended for use within our organization and should only be shared on a need-to-know basis. It's important to maintain the confidentiality of this data to protect our operational effectiveness.

2. Storage:

Internal data should be stored in secure systems with appropriate access controls, including password protection, to limit access to authorized personnel only. Regular backups should also be performed to ensure data recovery in case of loss or damage.

3. Transmission:

When internal data needs to be transmitted, it should ideally be sent via secured, authenticated channels. While encryption isn't mandatory for this classification, using encrypted channels when available adds an extra layer of protection.

4. Retention and Disposal:

Internal data should be retained as per the organization's data retention schedule. As a guideline, internal data should typically be retained for a minimum of three years, in compliance with general business practices. However, different types of internal data might have different retention requirements. For instance, any internal data related to payments, inline with PCI DSS, should be retained for a minimum of one year but must not contain any sensitive cardholder data.

Following the designated retention period, data should be archived for an additional two years in a secure environment, after which, if there are no legal, regulatory, or business reasons for further retention, it can be securely deleted.

This policy outlines the proper handling of internal data in our organization. By adhering to it, we can maintain the confidentiality of our internal operations and comply with necessary regulations and standards.

Internal data is information meant for internal use within our organization and not intended for public disclosure. Examples may include administrative details, operational schedules, internal communications, and meeting minutes. While the disclosure of internal data is not as damaging as confidential or sensitive data, it still requires proper management for operational effectiveness.

Policy:

1. Usage: Internal data should only be used for organization-related activities and decision-making processes.
2. Sharing: Internal data should be shared only with authorized employees who need the data to fulfill their job responsibilities.
3. Security: Basic security measures such as password protection and secure network access should be in place to protect internal data from unauthorized access, alteration, or deletion.

Procedure:

1. Access Control: Permissions should be assigned based on roles within the organization. Each employee should have access only to the internal data that they need for their role.
2. Storage: Internal data should be stored on secure organization servers with access control in place. Use of personal storage devices or non-secure cloud storage for storing internal data should be prohibited.
3. Transmission: Internal data should be transmitted only through secure, authenticated channels. Use of non-secure channels such as personal email for sending internal data should be avoided.
4. Data Lifespan Management: Internal data that is no longer needed should be securely disposed of to prevent unauthorized access or misuse. A regular review process should be in place to identify such data.
5. Incident Reporting: Any suspected or actual breach involving internal data should be promptly reported to the organization's designated security officer or team.

Confidential Data Handling Policy and Procedure

1. Handling:

Confidential data is a type of data that includes personal information, such as the details of our students and donors, and any proprietary information. The handling of such data requires extra vigilance. Only authorized individuals should access it and share it strictly on a need-to-know basis. Unauthorized access, disclosure, or usage of confidential data is strictly prohibited and can result in disciplinary action.

2. Storage:

When it comes to storage, confidential data must be protected by strong security measures. This includes the use of encryption, rigorous access control mechanisms, and regular audits of access logs. Confidential data must be stored on our organization's secure servers or approved encrypted storage solutions to prevent unauthorized access.

3. Transmission:

Transmission of confidential data must be done over secure, authenticated, and encrypted channels. Emails containing confidential data should be encrypted, and large data files should

be transferred via secure, encrypted transfer protocols. Confidential data should never be transmitted over public Wi-Fi networks without using a secure, encrypted connection (like a VPN).

4. Retention and Disposal:

The retention of confidential data should align with the organization's data retention policy and legal requirements. In line with PCI DSS and other relevant regulations, confidential data linked to payment transactions should be retained for a minimum of one year. However, sensitive cardholder data must never be stored after the authorization process.

After the required retention period, confidential data should be archived securely for an additional two years. Following this, if there is no ongoing business, legal, or regulatory requirement for keeping the data, it should be securely disposed of. This disposal should be carried out in a manner that prevents its reconstruction and subsequent unauthorized access or use.

Sensitive Data Handling Policy and Procedure

1. Handling:

Sensitive data, such as credit card numbers, bank details, and Social Security Numbers of students and donors, requires the highest level of protection. It should only be accessed by specifically authorized personnel and is never shared unless required by law enforcement or as per a legal directive. The unauthorized access, disclosure, or usage of sensitive data is strictly prohibited and can result in severe penalties, including termination of employment.

2. Storage:

Sensitive data must be stored in encrypted form, with rigorous access control mechanisms in place. Per the PCI DSS requirements, cardholder data must never be stored unless it's necessary to meet the needs of the business. If it is stored, stringent protective measures should be in place, including encryption and limited access. Also, sensitive authentication data must not be stored after authorization, even if encrypted.

3. Transmission:

Transmission of sensitive data must only be done over secure, authenticated, and encrypted channels. All cardholder data transmitted over open, public networks should be encrypted per the PCI DSS requirements.

4. Retention and Disposal:

The retention period for sensitive data should be as brief as possible and in line with the legal, regulatory, and business requirements. According to PCI DSS, cardholder data must not be retained longer than required for business, legal, and/or regulatory purposes. After the necessary retention period, sensitive data must be securely deleted, ensuring the data cannot be recovered.

Sensitive data, if archived, should be stored in a secure and encrypted format and only for the duration required by legal, regulatory, or business needs. After this period, it should be securely deleted using methods that prevent data recovery.