Appendix B: Regulated Data Authorization Form

Please complete the form below and return to UNO Information Services (IS) Technical Support Services, EAB 104.

Date: _____

1. Your Information

Name: _____

Phone: _____

Email: _____

NU ID: _____

College/Department: _____

Dean/Divisional Leader: _____

2. Storage Device Information

(Submit one form per device)

IS provides a service for the storage of regulated data, known as the Regulated Data File Server, which meets the necessary technical requirements for those authorized to store it. If it is necessary to store your regulated data in an alternative location, you must explicitly state that below:

[ ] If authorized, I WILL store regulated data on the Regulated Data File Server. (if checked, please proceed to Section 3)
[ ] If authorized, I WILL NOT store regulated data on the Regulated Data File Server. Please state your reason and location where you would like to store regulated data:

Reason: _____

Location:
[ ] Server IP: _____ Hostname: _____
[ ] Workstation
[ ] Laptop
[ ] Other: _____

Location of Device: Building: _____ Room: _____

Owned by: [ ] UNO [ ] Self [ ] Other: _____

Technical Support Staff Information
If the device is UNO owned and is a workstation, laptop, USB drive, etc., then your primary technician must sign below to acknowledge your storage of regulated data. You as the user of this device are responsible for the security of the regulated data on it.

Regulated Data Storage Technical Requirements
IS provides an electronic storage location for regulated data that meets the necessary technical requirements for those authorized to store it. If it is necessary to store your regulated data in an alternative location, you must explicitly state that on this form.

The following technical requirements must be met once you are authorized to store regulated University data.

If you are storing regulated data on the IS-managed Regulated Data Storage System, the device (laptop, workstation, etc.) being used to access the data must meet the following requirements:

- Software patches: Auto updates must be enabled or critical patches must be applied within a timely manner of being released. If a critical update cannot be applied, then you must notify the Information Security Office at security@unomaha.edu.
- Current anti-virus and spyware software must be enabled and set to scan and receive definition updates daily.

- Local firewalls must be enabled and allow only necessary network traffic.
- When possible, devices such as servers, workstations, and laptops used to store regulated data or access the Regulated Data Storage System must use strong AES 128-bit encryption.
- Workstations, laptops, servers, portable devices, and any other devices used to electronically store regulated data or access it on the Regulated Data Storage System are subject to audits to ensure technology requirements are being met as deemed necessary by the Regulated Data Authorization Committee.
- Once a device is no longer being used by the person authorized to store regulated data on it or access data on the Regulated Data Storage System, a complete secure deletion of the device must be performed by or through the Information Security Office.

If you are NOT storing regulated data on the IS-managed Regulated Data Storage System, the device (laptop, workstation, etc.) being used to store must meet the following requirements, in addition to the requirements listed above:

- Regulated data cannot be stored on a device that directly accepts incoming connections from the Internet, such as a web server or other forward-facing service.
- The server will use Identity Finder to accurately inventory the contents of the system.
- Vulnerability scans will be performed on a regular basis on workstations and servers storing regulated data by the Information Security Office. Critical issues identified in the scan must be acted upon in a reasonable timeframe as deemed by the Information Security Office.
- Reasonable protective measures must be put in place to physically secure devices that store regulated data. These measures should prevent easy physical theft.
- Deletion of regulated data must be performed by a secure deletion tool.

If the device that you use to store regulated data on is a server, then the primary technician for that server is responsible for the security of the data on that device.

Primary Technician Support Staff Agreement
By signing below, I acknowledge that the requester is storing regulated data on a device in the area that I support. If the device is a server I manage, then I understand that I am responsible for protecting the regulated data on it.

Primary Technician Support Staff Signature: _____

Phone: _____ Email: _____

3. Regulated Data File Server Authorization

If seeking authorization to store regulated data on the IS-managed Regulated Data File Server, please complete the following section.

Department Name: _____
(This or a similar name will become the folder name on the Regulated Data File Server and the Active Directory (AD) group name which protects this folder.)

Users (UNO NetIDs) authorized to access this folder: _____
Person(s) Authorized (UNO NetIDs) to request membership changes to the AD group protecting this folder:

_____

4. Regulated Data Type

(Check all data types stored on the device. Report only University-owned Regulated Data. For example, if you store your own credit card information on your laptop, it does not apply.)

[ ] SSN
[ ] Bank Account Access *(bank account numbers, credit card numbers, etc.)*
[ ] Driver's/State License #
[ ] Username with Password *(username/ID number in combination with password/PIN that grants access to Regulated Data)*
[ ] Biometric Information

5. Can the device (laptop, workstation, etc.) being used to store regulated data OR access regulated data on the IS managed Regulated Data File Server be encrypted?

[ ] Yes
[ ] No
If no, please explain the reason here: _____

6. Your Business Need

(Please indicate your need to store this data)

7. Related Information

Resource	***Description***
http://www.nebraska.edu/docs/president/16%20Responsible%20Use%20of%20Computers%20and%20Info%20Systems.pdf	NU Executive Memorandum 16
http://nebraska.edu/docs/president/26%20Information%20Security%20Plan%20%28GLB%20Compliance%29.pdf	NU Executive Memorandum 26
http://uniweb.legislature.ne.gov/FloorDocs/99/PDF/Slip/LB876.pdf	Consumer Notification of Data Security Breach Act of 2006
https://www.pcisecuritystandards.org/	Payment Card Industry Data Security Standards (PCI DSS)

8. Employee Responsibilities

The following is the list of terms and conditions related to the electronic storage of regulated University data:

_____ I understand that I am responsible for protecting the regulated data that I electronically store.
(initials)

_____ I agree to receive training on how to securely store regulated data.
(initials)

_____ I agree to report all security violations to my supervisor immediately.
(initials)

_____ I understand that any violation of this agreement may be cause of disciplinary and, possibly, legal action.
(initials)

_____ I understand I will be subject to annual reauthorization which includes re-submission of this form on an annual
(initials) basis.

Employee:

By signing below, I am acknowledging that I have read and agree to the terms and conditions described in this form and I have read and agree to comply with the University policies governing the use, storage, and disposal of regulated data.

_____ _____
Signature Date

9. Authorization

Dean/Divisional Leader
This employee should be authorized to store regulated data on an electronic storage device as a necessary part of his/her job duties.

_____ _____
Signature Date

Regulated Data Authorization Committee
Approve or deny the request to store regulated data on an electronic storage device.

_____ _____
Signature Date

[ ] Approved
[ ] Denied for reason: _____

_____

_____