DEVELOPING A LONG-TERM PLAN FOR DATA MANAGEMENT

VION

A GUIDE FOR UNIVERSITIES

DATA MANAGEMENT IN HIGHER EDUCATION: WHAT TO CONSIDER & HOW TO GET STARTED

INTRODUCTION

The burden of managing and securing data for university administrators is continually growing – and keeping pace is a constant challenge. Not only are institutions obligated to store and protect personal data, they are also required to manage an increasing volume of research data. Where there is sensitive data, there is risk and every day there is more on the line. Looking across higher education at the data landscape many questions remain: Is your system safe, stable and built for the long haul? Does it have what you need to not only secure this data but also use it to help improve operations or understanding?

There is an innate value in stable storage, accessibility and reliability that extends beyond peace of mind to personal safety and the bottom line. The three main areas of focus universities should consider as they develop a data management program include: managing Personally Identifiable Information (PII), research data and the explosive growth of data across the institution.

1: GOOD DATA STEWARDSHIP FOR PERSONAL INFORMATION

Every student ID is a doorway to personal information that students entrust to administrators for safekeeping. And the stakes are high. In fact, colleges and universities are obligated under federal law to protect sensitive data for students. With the digitization of student records and PII comes the need to store and search through various types of data, but not all data plays by the same rules. Social security numbers and student transcripts may be managed against one set of policies but health records are subject to additional regulations under HIPAA law. There are new compliance regulations and statutes driving Records & Information Management (RIM), requiring institutions to report student statistics back to state and federal government agencies. Administrators are tasked with creating a system that properly protects the data sets according to the appropriate standards and policies.

> colleges and universities are obligated under federal law to protect sensitive data for students

Many of today's IT departments face an explosion in unstructured data with no effective means of managing it and all the responsibility of its stewardship. Currently only 5% of this content is valuable in its current state. With such a wealth of data available, it has to be searchable to be practical. PII gives leadership critical information on demographics and student populations that inform operations and policies. This information as well as statistics, grades, and research data often have to be reported back to government agencies to substantiate state funding, thereby making it critical for compliance.

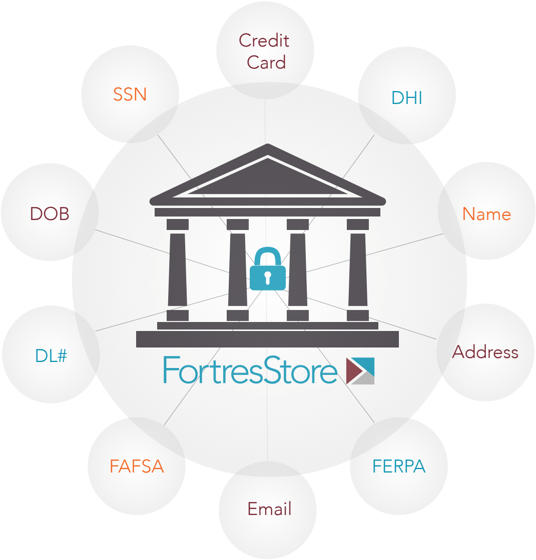
To best implement a privacy and data protection program, administrators should consider the following questions:

1. How do you currently manage electronic records, emails and information being sent over email?

2. How do you make this data accessible (where appropriate) to students, faculty and administrators?

3. How do you currently maintain compliance, meet retention period requirements and litigation preparedness as well as ensure data security and privacy?

4. What needs to change to make this process easier?



THERE IS AN INNATE VALUE IN **STABLE STORAGE, ACCESSIBILITY AND RELIABILITY** THAT EXTENDS BEYOND PEACE OF MIND TO PERSONAL SAFETY AND THE BOTTOM LINE.

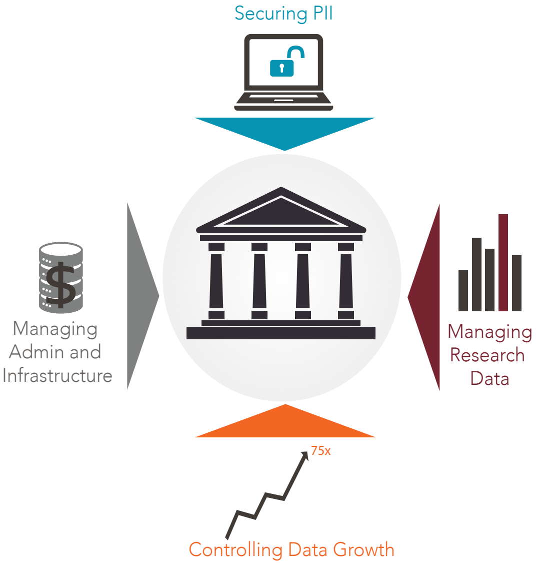
2: RESEARCH DATA — PROTECTING INTELLECTUAL PROPERTY & THE GRANT PIPELINE

Research funding can represent a significant percentage of a university's financial backbone. Just like PII, it has to be secure but accessible to serve the institution's needs. It often comes in many types, some data requires sharing externally with a wide audience, while other types require greater security. A centralized data management system is critical to ensuring proper storage and access by the right people at the right time, without overcomplicating the task.

Adopting a university-wide policy regarding research data management is important in serving the integrity of any research program. Safeguarding the program's assets is part of the organization's commitment and a means to perpetuate a healthy pipeline of grant funding for future projects. Applying best practices protects the university's intellectual, financial, human, and material investment in research. When institutions develop a responsible data management protocol, the resulting access to research data can also contribute to an improved public understanding of the university's contributions to the public good.

To be effective and compliant, a university's cyber infrastructure must support advanced data acquisition, storage, management, security, integration, mining, and visualization, as well as other information-processing services. Anything less can put an unnecessary financial burden on institutions as well as human resources – leaving universities vulnerable to risk in every place the data is stored. Eventually these seemingly small risks across the network can compromise what institutions work so hard to build.

Consider the common practice among research programs, which allows researchers to BYOD (Bring Your Own Device). This leaves universities with a significant data management and security burden. Administrators are tasked with reigning in these personal storage devices that typically are without documentation, version control, backup, or redundancy. For long-term stability, the infrastructure must now include systems for documenting, depositing, managing, archiving, and preserving data, facilitating efficient search and retrieval, and providing access. Having a centralized management system tackles the high-priority challenges for administrators.



Data Protection Challenges for Higher Education

THE EDUCATION SECTOR HAS THE SECOND HIGHEST PER CAPITA COST OF **CLEANING UP A DATA BREACH**, ESTIMATED AT $294 PER CAPITA.[1]

5 Things to Do in the Event of a Data Breach[2]

1. Higher a Forensics Team to Assess Damages
2. Contract for Legal Services
3. Notify Potential Victims
4. Develop a Public Relations Response
5. Harden Your Computer System

[1] *Taken from www.universitybusiness.com referencing a 2014 study from Ponemon Institute*

[2] *http://www.universitybusiness.com/article/hard-costs-data-breach*

3: MANAGING DATA GROWTH & STABILITY

Unstructured data is growing at a rate of 75% while structured data is growing at only 23%. Unstructured data includes email, images, video, social media, documents and more – and it is outpacing the growth of storage systems. Compounding this problem, many organizations must now retain content for longer periods of time in order to satisfy regulatory requirements. 90% of data is not accessed after 30 days but it retains tremendous value for big data down the line. The content itself is increasing in size as organizations store larger files, such as video recordings. For example, campus security video management alone accounts for an abundance of data under a university's care. It is important to centralize the storage and management of this information across a single or multiple campus locations to meet video retention requirements. The nature of video requires the capability and infrastructure to manage large files for defined time periods and policies to ensure it's done correctly. The costs of data storage and the means to make that palatable and practical for institutions is a growing need as data from dozens of sources is collected continuously at a record pace. It's a reality that requires action sooner rather than later.

A centralized single platform offers the security and versatility that institutions need to develop a truly long-term solution. Not only does it offer the storage, access and security profile institutions need, it also provides the flexibility to manage BYOD research programs and can centralize the collection of data from remote campuses, where organizations might not have the IT resources.

In the end, data managers and administrators across every industry agree: It's all about stability. In fact, most would sacrifice performance to have stability. But fortunately with the right solution administrators don't have to make sacrifices to gain that confidence.

4: MEET FORTRESSTORE

FortresStore was developed as a solution to the growing demands of data storage and security and is designed for organizations that need to manage volume with efficiency.

AUTOMATION

FortresStore automates the identification and collection of PII data, moving it to a centralized, secure repository. It removes the costly, manual process of collecting and moving data over a network – a process that is time-consuming and leaves universities exposed to hackers. Automation also reduces human error and produces cleaner, more accurate data. As PII grows, manual data movement becomes more complex and risky. FortresStore removes the complexity right from the start with the user experience. This process is seamless to the end user, allowing users to continue accessing data in the same way they always have without disruption.

> It removes the costly, manual process of collecting and moving data over a network – a process that is time-consuming and leaves universities exposed to hackers.

SEARCHABILITY/ACCESS

With FortresStore, administrators are able to search metadata for faster records retrieval and address the issue of personal devices in the research environment by centralizing management and placing data in a secure repository. Institutions that struggle with network bandwidth between remote and central campuses are also assured access and the same security.

Through the development of policies surrounding data management, administrators can maintain complete control over who has access to each type of data. This level of control and security ensures that institutional data remains in the possession of the institution and does not follow individuals when they leave.

End users, such as administration, faculty and staff, can securely access their data anytime, anywhere. Data managed within FortresStore is accessible using familiar tools such as Windows Explorer and Apple's Finder. Using FortresStore's mobile application, this data can also be retrieved via mobile devices allowing secure remote access to data.

MANAGING GROWTH

As institutions consider the path of their data management program, the focus is on building a system that flexes and changes as quickly as the data. With FortresStore, as data ages and is less likely to be accessed, it can be moved to free up primary storage for higher priority access. This allows administrators to set policy about storage tiers and automate the retention of data according to the university's pre-set timelines.

PREPAREDNESS & OPTIMIZING EXISTING TOOLS

FortresStore allows administrators to feel more confident and prepared in the event of disaster and the need to recover critical information. By providing the ability to move and save data to multiple locations, data is always accessible. This results in lower costs for back-up and recovery and also helps institutions meet backup and recovery SLAs more effectively.

Further, FortresStore bridges easily to cloud providers moving data to Private, Hybrid or Public cloud environments. Using automated policies, FortresStore can reduce administrative costs moving data to and from cloud providers such as Microsoft's Azure and Amazon's Web Services.

IN IT FOR THE LONG-HAUL

FortresStore is the long-term solution that sets you up to manage the growing data challenge and make it accessible and practical for institutions. It is the answer to the looming question that many administrators face when considering the stability and security of all the data across their ever-expanding network. Every minute the volume increases and the threats to data security get more sophisticated. FortresStore helps institutions take control and maintain control no matter how the world of data evolves in the future.

WHY ViON?

ViON has over 35 years of experience in managing and protecting data, meeting some of the most stringent requirements of government agencies and private enterprises. With ViON's approach, you are not locked in to a single technology or manufacturer; ViON can integrate the right solution into existing infrastructures to save time and money. ViON serves customers across the federal government, in the public sector including state and local government, education and health care, and commercial accounts.

ViON helps organizations rethink their data storage strategy, turning their data into information and unlocking new value, using industry-leading technologies that can include:

- Private cloud to provide dynamic, user directed, allocation of IT resources.
- Object storage to increase the flexibility of where data is stored, while increasing the knowledge of the data being stored.
- Leveraging disk cache to improve the user experience when accessing deep archive.
- Energy efficient tape and optical systems for long-term archiving.

ViON Headquarters
196 Van Buren Street
Herndon, Virginia 20170
(877) 857-ViON (8466)

www.vion.com