Security Plan

EE379K: Information Security and Privacy

Student Name: Zi Zhou Wang
Student EID: zw3948

1. Change History

This section reflects the changes made to the document.

Date	Description of Change	Change made by:
1/29/2018	Added purpose, audience, data inventory and appendix	Zi Zhou Wang
2/14/2018	Modified purpose, added information valuation and categorization, valuation and classification columns of appendix	Zi Zhou Wang
3/8/2018	Added Vulnerabilities and Risks and Matrix of vulnerabilities, and references	Zi Zhou Wang
4/1/2018	Added Trusted Identity for Information Access and Sharing Controls (Stakeholder types requiring access, Level of Assurance for Stakeholder Authentication, Stakeholder access control)	Zi Zhou Wang
4/15/2018	Added Incident Response Plan, Incident Identification, Incident Prioritization, Incident Response Team, Incident Response Playbook – Notification Plan	Zi Zhou Wang
5/3/2018	Added Information Security and Privacy, Trust Framework, Select Technology Solutions for your selected Trust Framework	Zi Zhou Wang

2. Purpose

As the CISO of The University of Utopia, I am responsible for the security and privacy of all data held by the University. One of the responsibilities of the CISO is to create and maintain a data inventory for their organization. As such, I am responsible for creating and maintaining a data inventory for The University of Utopia. The purpose of this document is to detail a potential security plan to protect that data and privacy of our students and faculty. This document will detail the data that needs to be protected, categorize and value the various pieces of data, identify all the potential risks to confidentiality, integrity, and availability, explain who can access the data for each data category. The audience description outlines who is meant to access the data inventory. It is imperative that the data inventory is accessed and used authorized users.

3. Audience

The data inventory of The University of Utopia is meant to be read by only those with the appropriate credentials to review the data elements held by the institution. These include the departments of the university who are responsible for the information, or the “owners” of the information. These include departments such as the registrar, directory, human resources, and the financial departments. Other patrons might include the vendors of the university, such as those working on construction or other services to the institution. Employees of the institution, or even staff who contribute to the database itself will also benefit from access to its information.

Overall, the data inventory of The University of Utopia serves as a summary of the institution. Information on what is available at the university, from course catalogs to student amenities are desired by prospective students. Likewise, its financial history and investments would be attractive to future investors who would like to partner with the institution. The audience of The University of Utopia’s data inventory is a very diverse group. Anyone who wished to interact with the institution would generally first seek information about it.

4. Data Inventory

Data inventory is the collection of data sources and elements of an institution. For the University of Utopia, its data inventory is crucial for the development of its business intelligence strategy. The university's data inventory includes detailed documentation of its data sources, their owners, where they're located, their value, and the importance. The data inventory exists so that all these elements are available in a usable format so that information of the institution can be used appropriately. Maintaining such a data inventory required a great deal of organization. Different departments within the university contribute data that must be processed and organized into a usable format. After this is done however, the data inventory of an institution is an invaluable record as a summary of informational assets.

5. Information Valuation and Categorization

The University of Utopia will classify its information assets into risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access. Risk classification is used primarily in ratemaking when there is not sufficient information to estimate a price for a given individual. In order to derive a price, individuals that are expected to have the same costs are grouped together. The actuary then calculates a price for the group and assumes that the price is applicable to all of the members of the group. Since the majority of data held by the University of Utopia do not have specified values, their values must be derived through estimation. As such, risk classification fits the model for developing a security plan for the protection of data held by the university.

In the Risk Based model of classifying information, data elements are classified into three categories: Low Risk, Moderate Risk, and High Risk. Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk. Low Risk data is intended for public disclosure, and the loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on the university's mission, safety, finances, or reputation. Data and systems are classified as Moderate Risk if they are not considered to be High Risk. Moderate Risk data are not generally available to the public and the loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on the university's mission, safety, finances, of reputation. Data and systems are classified as High Risk if the protection of the data is required by law or regulation. High Risk data is also data that the university is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed. Finally, High Risk data includes any information of which the loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on the university's mission, safety, finances, or reputation.

Valuation of data elements held by the University of Utopia will be determined through common black-market values of data elements when possible. For example, insurance information is typically worth $20 on black markets, while social security numbers are worth $30. Data elements that are easily accessible by the public are assigned $0. For example, a list of buildings owned by the university can be easily found on the university's website, and are hence worth $0. Miscellaneous elements that are not publicly available are priced based off their usefulness to data reports. For example, the demographics of students at the University would not be publicly available knowledge, but the publishing of such data could be sold to interested parties. As such, these types of data are prices based off their sensitivity. For example, the ethnicities of each student would be assigned a value of $1.

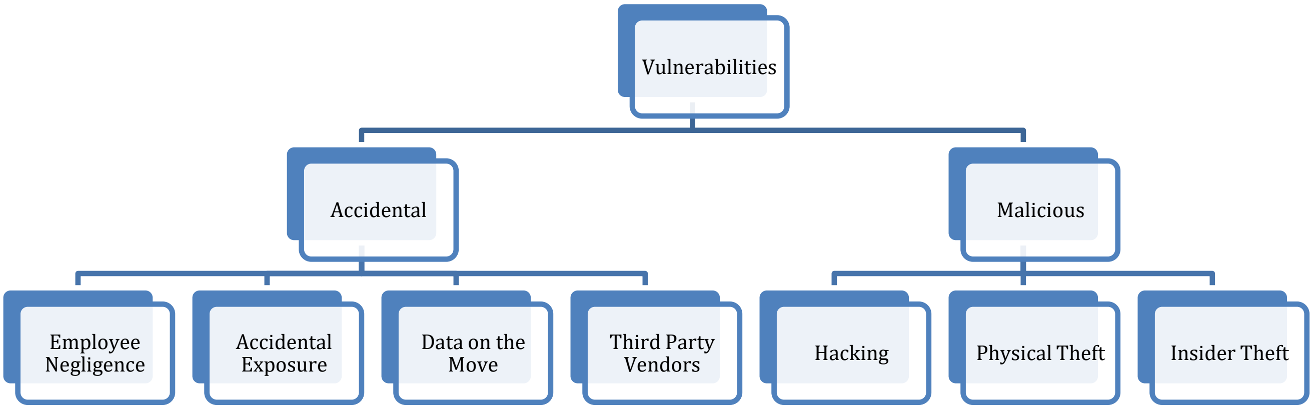
In the data inventory of The University of Utopia, 46% of data elements are Low Risk, 48% are Moderate Risk, and 6% are High Risk. In general, high value data such as insurance and bank information are classified in the High-Risk category. Information that are less sensitive, though not easily available to the public such as student IDs and registrar information are in the Moderate-Risk category. Finally, information that are easily accessed by the public are in the Low-Risk category. The general correlation between the classification categories and data valuation is that as Risk increases, so does the value of the data assets. For example, High Risk data elements are generally worth more than Moderate Risk elements, and Moderate Risk elements are generally worth more than Low Risk elements. Overall, the University of Utopia holds a wide range of data elements within its data inventory. The product of the number of data elements and the number of each element would amount to a surprising large financial sum. Data breaches of high risk data would be a financial and reputational disaster for the university.

6. Matrix of Vulnerabilities and Identification of Risks to Confidentiality, Integrity, and Availability

With industry compliancy and information security laws and mandates tightening, the need for conducting a vulnerability and risk assessment is now paramount. The University of Utopia must now be information security conscious and must develop and implement proper security controls based on the results of their internal risk assessment and vulnerability assessment. By conducting a risk assessment and vulnerability assessment, The University of Utopia would be able to uncover known weaknesses and vulnerabilities in its existing IT infrastructure, prioritize the impact of these vulnerabilities based on the value and importance of affected IT and data assets, and then implement the proper security controls and security countermeasures to mitigate those identified weaknesses. This risk mitigation results in increased security and less probability of a threat or vulnerability impacting the university's operating environment.

The ultimate goal of The University of Utopia is to prioritize its IT assets and IT infrastructure components to assess which IT assets should have their vulnerability reduced. Reducing vulnerability will assist the university in minimizing the potential risk and threats caused by vulnerabilities. The university will recognize that having an IT security architecture and framework consisting of policies, standards, procedures, and guidelines for their production IT systems, software, and applications is critical.

The matrix of vulnerabilities defines, identifies, and classifies the security holes (vulnerabilities) in a computer, communications infrastructure, or any other data network used by The University of Utopia. The matrix of vulnerabilities classifies vulnerabilities, describes specific vulnerabilities, analyzes the risk they pose, and assigns risk levels. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.



Top Risk impact examples:

- Hacking of university server – $44,000 per hour of the hack in progress. More serious hacks could take a week to recover from. A week worth of labor would cost around 5600 dollars = (7 days * 8-hour work day * $100 per hour).
- Stolen Server – Varies per data cost. The cost to replace and setup a new server (in event of something like an unrecoverable theft) costs around $13,500. In addition to cost. Assuming a backup is available it could take a day to restore the data which is around 800 dollars = (8-hour work day * $100 per hour).

Type of Vulnerability	**Description of specific vulnerability**	**Risk posed by vulnerability**	**Risk Level (high, medium, low)**
Hacking	Email phishing where users opens an email attachment that launches malware to allow hacker continued but undetected access to users' computer	Confidentiality - hacker is able to access and copy/transport information from users' computer Integrity – hacker access could permit hacker to change information on users' computer	High risk level for Confidentiality and Integrity – while risk level depends on the classification level of data on users' computer. Risk level is assigned based on highest possible level of data classification and associated risk
Physical Theft	Mail sent to the university could be stolen through either an insecure mail room, or through poor placement of delivery	Confidentiality – mail thief is able to access information from the university's mail Availability – mail thief could render information contained in mail unavailable to authorized users	High risk level for Confidentiality and Availability - sensitive information can be contained in mail
Third Party Vendors	Construction workers contracted by the university could leak building access codes to unauthorized parties	Confidentiality – contract worker could leak information to unauthorized parties	Medium risk level for confidentiality – building access codes should not be provided to unauthorized users, though severe damage is unlikely
Insider Theft	Research assistant from within the university sells unreleased research data	Confidentiality – research assistant gives unauthorized party access to the university's research data	Medium risk level for confidentiality – unpublished research topics are information that are not too dangerous for the university if exposed

Employee Negligence	The university registrar secretary sends documents to the wrong student, compromising the privacy of another student's information	Confidentiality – registrar secretary sends documents to an unauthorized party Availability – the student of whom the document was intended did not receive his document	Medium risk level of confidentiality and availability – student receives sensitive information, but is unlikely to act maliciously
Accidental Exposure	The university's research topics website accidentally releases topics of projects that have yet to be confirmed	Confidentiality – research topics that are not yet supposed to be public knowledge are released	Low risk level of confidentiality – un published research topics pose minimum risk to the university
Data on the Move	A laptop that contains past university research data is sold at an auction	Confidentiality – research data that was not supposed to be given freely was included in the purchase of the laptop	Low risk level of confidentiality – old research data can be purchased by the public
Insider Theft	Former university registrar employee accesses a database of student information, including social security number, of students seeking to apply for scholarships	Confidentiality – former employee accesses information that they had no authority to access	Hight risk level of confidentiality – theft of PII such as social security numbers are very high risk
Third Party Vendors	Financial firm that the university hired to review the university's finances refused to return the university's financial documents	Confidentiality – financial firm refused to relinquish access to the university's financial documents	Medium risk level of confidentiality – though restricted, the university's financial documents are unable to cause substantial damage to the university
Physical Theft	A server database of the university containing medical data of students and employees was stolen from the server room	Confidentiality – sensitive information contained on the server can be viewed by unauthorized parties Integrity – information changed, or modified by the thief Availability – information contained on the server might be the only copy held by the university	High risk level of confidentiality, integrity, and availability – sensitive information contained on the server can now be viewed and modified by unauthorized parties as well as being denied to authorized ones.

Employee Negligence	While advertising an explore the university event for middle schoolers, a university employee publishes unreleased research data as part of the advertisement campaign	Confidentiality – unpublished research information is made available to the public	Medium risk level of confidentiality – the premature release of research data could cause a minor competitive disadvantage
Accidental Exposure	The university's alumni website accidentally published the former student's social security numbers, address, phone numbers, and emails	Confidentiality – sensitive PII of former students is released to the public	High risk of confidentiality – as information that is very sensitive such as PII have been compromised
Employee Negligence	A university registrar employee falls victim to a phishing scam, revealing his username and password to the attacker without knowing it	Confidentiality – the attacker can use the obtained credentials to access unauthorized information Integrity – the attacker can use obtained credentials to change or modify unauthorized information Availability – the attacker can render certain data elements inaccessible with the stolen credentials	High risk of confidentiality, integrity and availability as - an attacker could have free reign on sensitive information using stolen credentials
Employee Negligence	Employee forgets to delete information used for a report before sending out the report to the public	Confidentiality – information that was not meant to be publicly available is now publicly available	Medium risk to confidentiality – though unintended, the release of information contained in a report is unlikely to cause substantial damage to the university
Employee Negligence	Employee accidentally deleted important information from a server	Availability – Access to the information is no longer available as it has been deleted by the employee	High risk to availability – depending on contents of data, but could be high risk

Employee Negligence	Programmer breaks access to data after pushing a bad update	Availability – Access to site or database is no longer available due to corrupted access credentials	Low risk to availability as credential programming can be easily revertible
Third Party Vendors	Employee information given for insurance reasons	Confidentiality – the vendors can view information even after the contract ends	There is a medium-high risk level involved as the chance of a third-party vendor holding on to information is high; however, real risk level varies depending on the classification level of the information given
Third Party Vendors	Current partnered vendors encounter have their own data breach	Confidentiality – the vendors can view information even after the contract ends	There is a medium-high risk level involved as the chance of a third-party vendor holding on to information is high; however, real risk level varies depending on the classification level of the information given
Insider Theft	Disgruntled employee destroys data out of vengeance	Integrity – The employee could modify the information Availability – The employee could destroy the information making it unavailable	There is a medium risk level involved for both classifications of information have employees assigned to access it, but the chance of it occurring is fairly low.
Insider Theft	Employee is bribed by a competitor to steal/modify information	Confidentiality – The employee could leak information to unauthorized parties	Medium risk level as it is a fairly rare occurrence but information could be fairly sensitive.
Insider Theft	Employee sensitive knowledge of the company leaves (legally) and reveals inner information.	Confidentiality – The employee could leak information to unauthorized parties	Medium risk level as it is a fairly rare occurrence but information could be fairly sensitive.

Hacking	Employee installs software that logs entered information on the computer.	Confidentiality – The employee could leak information to unauthorized parties	High risk level as it is a fairly rare occurrence but the amount of damage is very high should it occur.
Insider Theft	Employee adds access for third party vendors to access from.	Confidentiality – The employee could leak information to unauthorized parties Integrity – Depending on the type of access, data can be modified	High risk level as it is a fairly rare occurrence but the amount of damage is very high should it occur.
Physical Theft	A thief steals university hardware that contains information.	Confidentiality – a thief does not have authorized access	There is a medium risk level associated with confidentiality as the chance of this happening is not too uncommon.
Physical Theft	A thief destroys data in the process of theft	Integrity – data is destroyed in the process of the theft	It is a low-level risk to integrity as a theft most likely would not lead to destruction of data.
Data on the Move	Data could be left on University owned hardware. If the data is not removed from the source if it is ever resold, it is effectively leaked.	Confidentiality – The party that buys our hardware is most likely not authorized to access the data.	There is a low risk level associated. There is a low chance of this situation occurring, and even if it did the classification level of the data located is probably fairly low.
Hacking	Data could be left on University owned hardware. If the data is not removed from the source if it is ever resold, it is effectively leaked.	Confidentiality – The party that buys our hardware is most likely not authorized to access the data.	There is a low risk level associated. There is a low chance of this situation occurring, and even if it did the classification level of the data located is probably fairly low.

7. Trusted Identity for Information Access and Sharing Controls

Access Control Design

The University of Utopia will employ Role-Based Access Control (RBAC). Role-based access control restricts network access based on a person's role within the university. Parties are only allowed to access the information necessary to effectively perform their duties. Access will be based on several factors such as authority, responsibility, and job competency. In addition, access to computer resources can be limited to specific tasks such as the ability to view, create or modify a file. As a result, sensitive data is restricted to those who lack the authorization. This is especially helpful in an environment such as a university where there are many employees, students and third-party contractors who make it difficult to closely monitor information and network access.

Stakeholder types requiring access

Type of Stakeholder	**Description of the Stakeholder (include the activities this stakeholder may perform requiring their information access and authorizations)**
Students	Students may access university databases that contain information relevant to their studies by providing surface level authentication. Students can for example, check their grades or secure academic notes. More sensitive information pertaining to the specific student such as academic and personal records are also accessible by students, though with the requirement of a more involved authentication process.
Staff	The staff of the university holds access rights that are standard for employees. These include access to their employment information such as payment and shift history. For example, staff of the university can check their payment history and shift schedule. To access this information, staff would need to provide basic proof of identity.
Faculty	Faculty require access to higher authorization databases such as student grades and academic administration. For example, faculty can change student grades or send secure academic notes. In addition, faculty should have access to all information and databases that are available to a staff member.
Administrators	Administrators have access to the most sensitive information available to the university such as the personal information of students, staff and faculty to perform their duties. For example, administrators can check sensitive personal information such as university security questions of staff and students. As such, administrators require the highest level of authentication as their access has the highest risk if compromised.
Alumni	Alumni can access special alumni databases that are not available to the public. For example, alumni can check the schedule of special alumni events planned by the university. Information available on these databases however, are of low risk. As such, alumni require low levels of authentication to access information available to them.
Parents	Parents of students have access to student grades, as well as basic administrative privileges that are available to students. Parents can for example, check the grades of dining funds of a student. As such, the authentication of parents should be strong, but weaker than that of students.

Visitors	Visitors of the university have access to publicly available data that the university releases. For example, they may check the university events scheduled for a given week or check the prices of football tickets. As such, very low levels of authentication are needed for visitors.

Level of Assurance for Stakeholder Authentication

Type of Stakeholder	Classification for Information Accessed (see Section 5)	IAL	TAL	LOA	Justification for Assignment of Assurance Levels
Students	High Risk	4	4	4	Students have access to sensitive information such as personal information that pertains to themselves and secure academic information. As such, highest levels of identity assurance, token assurance and overall level of assurance is required.
Staff	High Risk	4	4	4	Staff have access to sensitive information that pertains to their employment information. These include personal identifiable information and others that are highly restricted. As such, highest levels of identity assurance, token assurance and overall level of assurance is required.
Faculty	High Risk	4	4	4	Faculty have access to sensitive information such as student grades, secure academic information as well as all those available to staff. As such, highest levels of identity assurance, toke assurance and overall level of assurance is required.
Administrator	High Risk	4	4	4	Administrators have access to the highest risk elements of the university such as PII of all students, faculty, and staff. As such, highest levels of identity assurance, token assurance and overall level of assurance is required.
Alumni	Medium Risk	2	2	2	Alumni have access to information that are not available to the public. However, these data elements are not sensitive and have low risk to the university if disclosed. As such, some confidence in identity assurance, token assurance and overall level or assurance is sufficient.
Parents	Medium	3	3	3	Parents have access to information about their student's grades and dining funds. Though these data elements are restricted to the public, they are unlikely to cause sufficient

					harm to the university if compromised. As such, high confidence in identity assurance, token assurance and overall level of assurance is sufficient.
Visitors	Low Risk	1	1	1	Visitors only have access to information and data elements that are already available to the public. As such, low confidence in identity assurance, token assurance and overall level of assurance is sufficient.

Stakeholder access control

Type of Stakeholder	**Access Control Specification**	**Access Control Specification applies to what part of the Information Inventory.**
Students	**Designation (Role based)** **If (person is student)** **Then grant access to:** Student graduation date Student graduation plan Student hours taken Student leave status Student leave reason Student race/ethnicity Student special program status Student university ID Student home address Student local address Student phone number Student personal email address Student university email address Student GPA Student social security number Student university login password Student date of birth Student current class schedule Student citizenship information Student disciplinary records Student insurance provider Student insurance ID Student emergency contact person Student emergency contact phone number Student emergency contact email address Student gender Student agreements Student Past Education	Student graduation date Student graduation plan Student hours taken Student leave status Student leave reason Student race/ethnicity Student special program status Student university ID Student home address Student local address Student phone number Student personal email address Student university email address Student GPA Student social security number Student university login password Student date of birth Student current class schedule Student citizenship information Student disciplinary records Student insurance provider Student insurance ID Student emergency contact person Student emergency contact phone number Student emergency contact email address Student gender Student agreements Student Past Education List of course information

	List of course information Course instructors' names Course names Course numbers Course section numbers Course days Course beginning hour Course ending hour Course building number Course room number Course number of students Course sequence number Course record type	Course instructors' names Course names Course numbers Course section numbers Course days Course beginning hour Course ending hour Course building number Course room number Course number of students Course sequence number Course record type
Staff	**Designation (Role based)** **If (person is staff)** **Then grant access to:** Employee first name Employee last name Employee Gender/Race Employee date of birth Employee address Employee email address Employee phone number Employee gender Employee veteran status Employee payment information Employee checking information Employee insurance information Employee agreements	Employee first name Employee last name Employee Gender/Race Employee date of birth Employee address Employee email address Employee phone number Employee gender Employee veteran status Employee payment information Employee checking information Employee insurance information Employee agreements
Faculty	**Designation (Role based)** **If (person is faculty)** **Then grant access to:** Professors employment history Professors criminal records Professors social security number Professor race/ethnicity Professor salary Professor university ID Professor home address Professor local address Professor phone number Professor personal email address Professor university email address Years professor has taught Professor retirement benefits Professor university login password Professor date of birth	Professors employment history Professors criminal records Professors social security number Professor race/ethnicity Professor salary Professor university ID Professor home address Professor local address Professor phone number Professor personal email address Professor university email address Years professor has taught Professor retirement benefits Professor university login password Professor date of birth List of current professors Professor citizenship information List of past professors

	List of current professors Professor citizenship information List of past professors Professor insurance benefits Professor insurance number Professor Gender Professor Teaching Experience	Professor insurance benefits Professor insurance number Professor Gender Professor Teaching Experience
Administrator	**Designation (Role based)** **If (person is administrator)** **Then grant access to:** List of current students List of past students Current employee list Past employee list Employee Education Total university revenue University cash holdings University accounts receivable University inventory University prepaid expenses University investments University equipment inventory University accumulated depreciation equipment University total assets University total equity University total stock holder's equity University accounts payable University accrued expenses payable University bonds payable University common stock University retained earnings University balance sheet University income statement University sales revenue University cost of goods sold University operating expenses University depreciation expenses University tax expense University interest expense University loss on disposal of assets University donation income University government funding income University financial aid payments University land worth History of investments History of income	List of current students List of past students Current employee list Past employee list Employee Education Total university revenue University cash holdings University accounts receivable University inventory University prepaid expenses University investments University equipment inventory University accumulated depreciation equipment University total assets University total equity University total stock holder's equity University accounts payable University accrued expenses payable University bonds payable University common stock University retained earnings University balance sheet University income statement University sales revenue University cost of goods sold University operating expenses University depreciation expenses University tax expense University interest expense University loss on disposal of assets University donation income University government funding income University financial aid payments University land worth History of investments History of income History of expenses

	History of expenses List of university graduate students List of university undergraduate students List of university doctoral students List of university researchers List of university post-doctoral List of university research topics List of university research progress List of university research approvals List of university research denials List of university research resource allocation List of past university research topics List of past university research contributions List of past university research progress List of university alumni List of contributions made by university research List of contributions made by university alumni University awards List of university majors List of university advisors List of university scholarship applicants List of university approves scholarship applicants List of approves university scholarship amounts	List of university graduate students List of university undergraduate students List of university doctoral students List of university researchers List of university post-doctoral List of university research topics List of university research progress List of university research approvals List of university research denials List of university research resource allocation List of past university research topics List of past university research contributions List of past university research progress List of university alumni List of contributions made by university research List of contributions made by university alumni University awards List of university majors List of university advisors List of university scholarship applicants List of university approves scholarship applicants List of approves university scholarship amounts
Alumni	**Designation (Role based)** **If (person is alumni)** **Then grant access to:** List of university alumni List of contributions made by university alumni Notable alumni athletes	List of university alumni List of contributions made by university alumni Notable alumni athletes
Parents	**Designation (Role based)** **If (person is alumni)** **Then grant access to:** Student graduation date Student graduation plan Student hours taken Student leave status Student leave reason Student race/ethnicity	Student graduation date Student graduation plan Student hours taken Student leave status Student leave reason Student race/ethnicity Student special program status Student university ID Student home address

	Student special program status Student university ID Student home address Student local address Student phone number Student personal email address Student university email address Student GPA Student social security number Student university login password Student date of birth Student current class schedule Student citizenship information Student disciplinary records Student insurance provider Student insurance ID Student emergency contact person Student emergency contact phone number Student emergency contact email address Student gender Student agreements Student Past Education List of course information Course instructors' names Course names Course numbers Course section numbers Course days Course beginning hour Course ending hour Course building number Course room number Course number of students Course sequence number Course record type	Student local address Student phone number Student personal email address Student university email address Student GPA Student social security number Student university login password Student date of birth Student current class schedule Student citizenship information Student disciplinary records Student insurance provider Student insurance ID Student emergency contact person Student emergency contact phone number Student emergency contact email address Student gender Student agreements Student Past Education List of course information Course instructors' names Course names Course numbers Course section numbers Course days Course beginning hour Course ending hour Course building number Course room number Course number of students Course sequence number Course record type
Visitors	**Designation (Role based)** **If (person is visitor)** **Then grant access to:** Professor Education University buildings list University buildings zip codes University buildings shipping address University buildings ownership status University building construction date University building square feet University buildings replacement value University buildings physical status	Professor Education University buildings list University buildings zip codes University buildings shipping address University buildings ownership status University building construction date University building square feet University buildings replacement value University buildings physical status University buildings functional status

	University buildings functional status University campus list List of university rooms List of university room types List of university room square feet List of university number of rooms University room type summary University coordination agencies University space utilization University building number University building residential classification University buildings cost of latest renovation University buildings year of latest renovation University buildings air conditioning status University buildings number of floors University buildings last year of record update University buildings assignable and accessible area University no assignable, circulation and building service areas University parking structures University inventory data University room inventory University rooms and space definitions University rooms primary use University phantom walls and prorations University unclassified facilities University classification of rooms University room data elements collected University room data elements definitions University classroom facilities University laboratory facilities University office facilities University study facilities University special use facilities University general use facilities University support facilities University health care facilities University residential facilities University unclassified area University unassignable area University structural area List of university athletes List of university sponsored sports List of university coaches List of university sports teams	University campus list List of university rooms List of university room types List of university room square feet List of university number of rooms University room type summary University coordination agencies University space utilization University building number University building residential classification University buildings cost of latest renovation University buildings year of latest renovation University buildings air conditioning status University buildings number of floors University buildings last year of record update University buildings assignable and accessible area University no assignable, circulation and building service areas University parking structures University inventory data University room inventory University rooms and space definitions University rooms primary use University phantom walls and prorations University unclassified facilities University classification of rooms University room data elements collected University room data elements definitions University classroom facilities University laboratory facilities University office facilities University study facilities University special use facilities University general use facilities University support facilities University health care facilities

	List of university sports team members University sports championships Notable alumni athletes Academic standing of athletes Football team record Number of injuries Number of home games Number of away games Number of playoff runs Deepest playoff runs Number of years since last championship MVP of each year Longest game	University residential facilities University unclassified area University unassignable area University structural area List of university athletes List of university sponsored sports List of university coaches List of university sports teams List of university sports team members University sports championships Notable alumni athletes Academic standing of athletes Football team record Number of injuries Number of home games Number of away games Number of playoff runs Deepest playoff runs Number of years since last championship MVP of each year Longest game

8. Incident Response Plan

Incident Identification

In the world of data security, an event is event as “any observable occurrence in a system or network,” such as sending an e-mail message or a firewall blocking an attempt to connect. A security or privacy incident, on the other hand, is, an event that violates an organization’s security or privacy policies involving sensitive information such as social security numbers or confidential medical information. Data breach is a security (or privacy) incident that meets specific legal definitions as per state and federal breach laws. Data breaches require notification to the affected individuals, regulatory agencies, and sometimes credit reporting agencies and the media. Only a small percentage of privacy or security incidents escalate into data breaches but to identify them there’s a regulatory obligation to conduct an incident risk assessment when the incident evolves PHI or PII.

Events

Name of Events	**Description of Event**	***Possible Loss – data, finances, time, reputation.**	**Concern for Business Continuity (would any portion of the business operations be impacted?)**
Sending an unauthorized e-mail message	Sending of unauthorized or classified data through an e-mail message.	Sensitive information might be lost, as well as reputational damage to the university if the loss is publicized.	Depending on the scope of the data breach, certain departments might have to take actions to recover of alleviate damaged caused by the event.
Firewall blocking an authorized attempt to connect	An authorized affiliate of the university’s attempt to connect is blocked by the firewall.	Along with the time of the authorized affiliate, the university’s IT department will also have to take time to fix the error in the firewall.	Depending on the role of the authorized affiliate, urgent functions of certain departments might be hindered or delayed.
Unauthorized use of system privileges	An unauthorized user has gained system privileges reserved for higher privileged users.	Data can be exposed to the unauthorized user, along with time to fix the error within the system and possible reputational damage if the event was to be publicized.	Depending on the maliciousness of the unauthorized user, business continuity can range from being unhindered to severely damage.
Unauthorized access to sensitive data	Sensitive data held by the university is accessed and viewed by unauthorized parties.	The loss of sensitive data such as student PII and financial records along with reputational damage are the primary concerns in this event.	The human resources and IT departments of the university will have to take measures to alleviate damages caused by the event.
Execution of malware that destroys data	Malicious malware is executed that caused the	Any and all data held by the university is at risk	Depending on the severity of data

	destruction of data held by the university.	from the destruction of data. Time from a range of university departments will have to be allocated to alleviate the event along with severe reputational damage.	destruction, departments might be able to carry out operations as normal or be completely shut down due to critical loss of valuable data.

Incidents

Name of Incident	Description of Incident	*Possible Loss – data, finances, time, reputation (descriptive	**Concern for Business Continuity (would any portion of the business operations be impacted?)
Lost thumb drive	Theft of equipment that contains sensitive information	Sensitive data will most likely be lost along with time required to mitigate damages, and possible reputational damages that might be incurred.	Depending on the data contained on the thumb drive, departments will have to act accordingly to take measurements in responding to the incident.
Brute force attack on system	A brute force attack on a client system results in a stolen password	A password is stolen which can cause further damage to the system's integrity if left unattended. Time from the IT department is necessary to correct the theft.	The department associated with the stolen password might have to restrict operations while the incident is taken care of.
Missing paper files	Paper files containing sensitive information are lost.	Sensitive information is lost through paper files, resulting in time from multiple different departments to respond, and possible reputational and revenue lost.	Departments associated with the files might have to delay operations while appropriate actions are done to alleviate the incident.
Phishing email	Employee opens phishing email and replies with confidential information	Confidential data is lost through the email. Time is required from departments involved to alleviate possible losses and damages.	The employee's department along with the IT department will have to take inventory and severity of the incident and act accordingly.
Loss of laptop	Theft of equipment that contains sensitive information	Sensitive data will most likely be lost along with time required to mitigate	Depending on the data contained on the laptop, departments will have to

		damages, and possible reputational damages that might be incurred.	act accordingly to take measurements in responding to the incident.

Breaches

Name of Breach	Description of Breach	*Possible Loss – data, finances, time, reputation	**Concern for Business Continuity (would any portion of the business operations be impacted?)
Student birthdates stolen	Database containing the birthdays of students are stolen by an unauthorized party.	With the compromise of student birthdates, the university registrar and IT departments will have to invest large amounts of time and suffer heavy reputational damages.	Student authorization across the university's system throughout departments would be compromised as a result of stolen student birthdates.
Student social security numbers stolen	Database containing the social security numbers of students are stolen by an unauthorized party.	With the compromise of student social security numbers, the university registrar and IT departments will have to invest large amounts of time and suffer heavy reputational damages.	Student authorization across the university's system throughout departments would be compromised as a result of stolen student social security numbers.
Confidential research data stolen	Database containing unpublished research data is accessed by an unauthorized party.	With the theft of confidential research data, the university's research department will suffer a substantial hit in trade secrets.	Though hindered, the research department of the university can still maintain operations as normal.
Student passwords stolen	Students passwords to the university system is stolen by an unauthorized party.	With the compromise of student system passwords, the university registrar and IT departments will have to invest large amounts of time and suffer heavy reputational damages.	Student authorization across the university's system throughout departments would be compromised as a result of stolen student passwords.
University scholarship funds account stolen	The financial account containing student scholarship funds is stolen by an unauthorized party.	The financial office along with the university IT department will lose substantial time and	The financial aid department will suffer heavy operational abilities as a result from this breach.

		reputation through the breach.	

Incident Prioritization

Incident Priority Level	***Criteria. Each criterion must account for combination of functional impact, information impact and recoverability.**	**Why? Justification for the criteria specification.**	**Example at occurrence at each level**
Level 1	(Functional Impact = NONE) AND (Business Impact = NONE) AND (Recoverability = REGULAR)	Lowest levels of functional impact, business impact, and recoverability requires the lowest classification of incident prioritization.	Designer of university website makes a typo.
Level 2	(Functional Impact = LOW) OR (Business Impact = PRIVACY BREACH) OR (Recoverability = SUPPLEMENTAL)	If any of functional impact, business impact, or recoverability requires more than the lowest levels, a slightly higher classification would be appropriate.	Printing network shuts down, rendering all university printers non-functional.
Level 3	(Functional Impact = MEDIUM) OR (Business Impact = PROPRIETAL BREACH) OR (Recoverability = EXTENDED)	If any of functional impact, business impact, or recoverability reach moderate categories of severity, then a moderate incident priority would be necessary to address the issue.	Unclassified proprietary information was accessed and exfiltrated
Level 4	(Functional Impact = HIGH) OR (Business Impact = INTEGRITY LOSS) OR (Recoverability = NOT RECOVERABLE)	If any of functional impact, business impact of recoverability is at critical risk, high level of incident prioritization is appropriate	University system has been completely shut down.
Level 5	(Functional Impact = HIGH) AND (Business Impact = INTEGRITY LOSS) AND (Recoverability = NOT RECOVERABLE)	Highest incident priority level involved the highest functional impact, business impact, and least recoverability.	Hackers attack the network, steal highly sensitive data including PII, then delete and shut down the network.

Incident Response Team

Incident Response Team Member Role	**Incident Response Team Member Responsibility**

Incident Lead	Identify, analyze, and correct hazards to prevent a future re-occurrence.
University President	Take care of logistical challenges within the university that requires higher authorization.
Technician	Bring forensic expertise to the team, determine or identify where the attack came from, how it was done, and what can be done to mitigate damages.
Communicator	Deal with personal relations within the team, make sure that communication within the team is clear and productive.
Legal Counselor	Provide legal expertise on the matter, advising the team's actions on their legal consequences.
Customer Service	Take care of customer calls or questions as they appear during an incident.
Human Resources	Deal with public image of the university, how the public is taking or understanding the incident, and respond in a way that helps the university's image.

Incident Response Playbook – Notification Plan

Incident	**Notify Who? Specify in terms of role**	**Notification Method**	**Notification Timing (usually specified in terms to upper limit time after the discovery, e.g. within 15 minutes of discovery)**
Level 1	Technician	E-mail	1 Day
Level 2	Technician, Communicator	E-mail (preferred) or call on phone	4 Hours
Level 3	Technician, Communicator, Customer Service	E-mail or call on phone (preferred)	1 Hour
Level 4	Technician, Communicator, Customer Service, Human Resources, Legal Counselor	Call on phone (preferred), or in person	10 Minutes
Level 5	University President, Students, Parents, Technician, Communicator, Legal Counselor, Customer Service, Human Resources, Staff, Faculty, Legal Counselor,	Call on phone, or in person (preferred)	Immediately

9. Information Security and Privacy

This section describes information security and privacy describing the system framework and technology serving as countermeasures to threats.

Trust Framework

The Centralized model is implemented in a client-server model. In this case, only the identity provider manages user identity storage and user authentication. All service providers use a unique identity provider. The Centralized model is suitable for the requirements of managing a lot of users, such as the requirements here at The University of Utopia. As far as convenience is concerned, the centralized model has an advantage as it allows user authentication through one service provider. Privacy issues however, might be as a concern as all identities are stores on only one identity provider. The centralized model is one of the more difficult to implement and complex models, however, its suitability to manage a large number of users will be worth the investment.

Select Technology Solutions for your selected Trust Framework

	Data Classification	**Technology or Design Principle**	**CIA Protection?**	**Rationale for selection of Technology or Method**
Data at Rest	All classifications of data	Least Privilege	Confidentiality Integrity Availability	Least privilege access control will help make sure that confidentiality, integrity and availability are preserved in university data at rest.
Data in Transit	All classifications of data	Data Encryption Standard (DES)	Confidentiality	DES encryption will make sure the university data cannot be viewed by unauthorized parties during transit.

Access to Data	All classifications of data	Complete Mediation	Confidentiality Availability	Complete mediation at every access to university data will help assure that only those who have access will view the data and decrease chances of attacks on university data.

10.Appendix A: Enterprise Information

Data Element	Location	Owner	Valuation	Classification
Student graduation date	Registrar database	University registrar	$1	Moderate Risk
Student graduation plan	Registrar database	University registrar	$1	Moderate Risk
Student hours taken	Registrar database	University registrar	$1	Moderate Risk
Student leave status	Registrar database	University registrar	$1	Moderate Risk
Student leave reason	Registrar database	University registrar	$1	Moderate Risk
Student race/ethnicity	Directory database	University directory	$1	Moderate Risk
Student special program status	Directory database	University directory	$30	High Risk
Student university ID	Directory database	University directory	$5	Moderate Risk
Student home address	Directory database	University directory	$5	Moderate Risk
Student local address	Directory database	University directory	$5	Moderate Risk
Student phone number	Directory database	University directory	$5	Moderate Risk
Student personal email address	Directory database	University directory	$1	Low Risk
Student university email address	Registrar database	University registrar	$5	Moderate Risk
Student GPA	Registrar database	University registrar	$5	Moderate Risk
Student social security number	Directory database	University directory	$30	High Risk
Student university login password	Directory database	University directory	$10	High Risk
Student date of birth	Directory database	University directory	$11	Moderate Risk
Student current class schedule	Registrar database	University registrar	$1	Moderate Risk
Student citizenship information	Directory database	University directory	$1	High Risk
Student disciplinary records	Office of dean of students' database	University dean of students' office	$1	Moderate Risk
Student insurance provider	Registrar database	University registrar	$20	High Risk
Student insurance ID	Registrar database	University registrar	$5	High Risk
List of current students	Registrar database	University registrar	$5	Moderate Risk

List of past students	Registrar database	University registrar	$5	Moderate Risk
Professors employment history	Human resources database	University human resources	$5	Moderate Risk
Professors criminal records	Human resources database	University human resources	$30	High Risk
Professors social security number	Human resources database	University human resources	$30	High Risk
Professor race/ethnicity	Human resources database	University human resources	$5	Moderate Risk
Professor salary	Human resources database	University human resources	$0	Low Risk
Professor university ID	Human resources database	University human resources	$5	Moderate Risk
Professor home address	Human resources database	University human resources	$5	Moderate Risk
Professor local address	Human resources database	University human resources	$5	Moderate Risk
Professor phone number	Human resources database	University human resources	$5	Moderate Risk
Professor personal email address	Human resources database	University human resources	$5	Low Risk
Professor university email address	Registrar database	University registrar	$5	Moderate Risk
Years professor has taught	Registrar database	University registrar	$0	Low Risk
Professor retirement benefits	Human resources database	University human resources	$5	Moderate Risk
Professor university login password	Registrar database	University registrar	$5	Moderate Risk
Professor date of birth	Human resources database	University human resources	$11	Moderate Risk
List of current professors	Registrar database	University registrar	$0	Low Risk
Professor citizenship information	Human resources database	University human resources	$5	Moderate Risk
List of past professors	Registrar database	University registrar	$0	Low Risk
Professor insurance benefits	Human resources database	University human resources	$20	Moderate Risk
Professor insurance number	Human resources database	University human resources	$20	High Risk
Student emergency contact person	Directory database	University directory	$1	Moderate Risk
Student emergency contact phone number	Directory database	University directory	$1	Moderate Risk

Student emergency contact email address	Directory database	University directory	$1	Moderate Risk
Current employee list	Human resources database	University human resources	$5	Moderate Risk
Past employee list	Human resources database	University human resources	$5	Moderate Risk
Employee first name	Human resources database	University human resources	$5	Moderate Risk
Employee last name	Human resources database	University human resources	$5	Moderate Risk
Employee date of birth	Human resources database	University human resources	$11	Moderate Risk
Employee address	Human resources database	University human resources	$5	Moderate Risk
Employee email address	Human resources database	University human resources	$5	Moderate Risk
Employee phone number	Human resources database	University human resources	$5	Moderate Risk
Employee gender	Human resources database	University human resources	$1	Low Risk
Student gender	Directory database	University directory	$1	Low Risk
Professor gender	Human resources database	University human resources	$1	Low Risk
Employee race/gender	Human resources database	University human resources	$1	Low Risk
Professor education	Human resources database	University human resources	$1	Low Risk
Employee education	Human resources database	University human resources	$1	Moderate Risk
Student past education	Directory information	University directory	$1	Moderate Risk
Professor teaching experience	Human resources database	University human resources	$0	Low Risk
Employee veteran status	Human resources database	University human resources	$1	Moderate Risk
Total university revenue	Financial database	University financial office	$50	Moderate Risk
Employee payment information	Human resources database	University human resources	$300	High Risk
Employee checking information	Human resources database	University human resources	$300	High Risk
Employee insurance information	Human resources database	University human resources	$20	High Risk
Student agreements	Directory database	University directory	$5	Moderate Risk
Employee agreements	Human resources database	University human resources	$5	Moderate Risk
University cash holdings	Financial database	University financial office	$100	Moderate Risk

University accounts receivable	Financial database	University financial office	$100	Moderate Risk
University inventory	Financial database	University financial office	$100	Moderate Risk
University prepaid expenses	Financial database	University financial office	$100	Moderate Risk
University investments	Financial database	University financial office	$100	Moderate Risk
University equipment inventory	Financial database	University financial office	$100	Moderate Risk
University accumulated depreciation equipment	Financial database	University financial office	$100	Moderate Risk
University total assets	Financial database	University financial office	$100	Moderate Risk
University total equity	Financial database	University financial office	$100	Moderate Risk
University total stock holder's equity	Financial database	University financial office	$100	Moderate Risk
University accounts payable	Financial database	University financial office	$100	Moderate Risk
University accrued expenses payable	Financial database	University financial office	$100	Moderate Risk
University bonds payable	Financial database	University financial office	$100	Moderate Risk
University common stock	Financial database	University financial office	$100	Moderate Risk
University retained earnings	Financial database	University financial office	$100	Moderate Risk
University balance sheet	Financial database	University financial office	$100	Moderate Risk
University income statement	Financial database	University financial office	$100	Moderate Risk
University sales revenue	Financial database	University financial office	$1	Low Risk
University cost of goods sold	Financial database	University financial office	$1	Low Risk
University operating expenses	Financial database	University financial office	$1	Low Risk
University depreciation expenses	Financial database	University financial office	$100	Moderate Risk
University tax expense	Financial database	University financial office	$0	Low Risk
University interest expense	Financial database	University financial office	$0	Low Risk
University loss on disposal of assets	Financial database	University financial office	$0	Low Risk

University donation income	Financial database	University financial office	$100	Moderate Risk
University government funding income	Financial database	University financial office	$100	Moderate Risk
University financial aid payments	Financial database	University financial office	$100	Moderate Risk
University land worth	Financial database	University financial office	$0	Low Risk
History of investments	Financial database	University financial office	$0	Low Risk
History of income	Financial database	University financial office	$0	Low Risk
History of expenses	Financial database	University financial office	$0	Low Risk
University buildings list	Facility services database	Facilities services office	$0	Low Risk
University buildings zip codes	Facility services database	Facilities services office	$0	Low Risk
University buildings shipping address	Facility services database	Facilities services office	$0	Low Risk
University buildings ownership status	Facility services database	Facilities services office	$100	Moderate Risk
University building construction date	Facility services database	Facilities services office	$0	Low Risk
University building square feet	Facility services database	Facilities services office	$0	Low Risk
University buildings replacement value	Facility services database	Facilities services office	$0	Low Risk
University buildings physical status	Facility services database	Facilities services office	$0	Low Risk
University buildings functional status	Facility services database	Facilities services office	$0	Low Risk
University campus list	Facility services database	Facilities services office	$0	Low Risk
List of university rooms	Facility services database	Facilities services office	$0	Low Risk
List of university room types	Facility services database	Facilities services office	$0	Low Risk
List of university room square feet	Facility services database	Facilities services office	$0	Low Risk
List of university number of rooms	Facility services database	Facilities services office	$0	Low Risk
University room type summary	Facility services database	Facilities services office	$0	Low Risk

University coordination agencies	Facility services database	Facilities services office	$0	Low Risk
University space utilization	Facility services database	Facilities services office	$0	Low Risk
University building number	Facility services database	Facilities services office	$0	Low Risk
University building residential classification	Facility services database	Facilities services office	$0	Low Risk
University buildings cost of latest renovation	Facility services database	Facilities services office	$0	Low Risk
University buildings year of latest renovation	Facility services database	Facilities services office	$0	Low Risk
University buildings air conditioning status	Facility services database	Facilities services office	$0	Low Risk
University buildings number of floors	Facility services database	Facilities services office	$0	Low Risk
University buildings last year of record update	Facility services database	Facilities services office	$0	Low Risk
University buildings assignable and accessible area	Facility services database	Facilities services office	$0	Low Risk
University no assignable, circulation and building service areas	Facility services database	Facilities services office	$0	Low Risk
University parking structures	Facility services database	Facilities services office	$0	Low Risk
University inventory data	Facility services database	Facilities services office	$0	Low Risk
University room inventory	Facility services database	Facilities services office	$0	Low Risk
University rooms and space definitions	Facility services database	Facilities services office	$0	Low Risk
University rooms primary use	Facility services database	Facilities services office	$0	Low Risk
University phantom walls and prorations	Facility services database	Facilities services office	$0	Low Risk
University unclassified facilities	Facility services database	Facilities services office	$0	Low Risk

University classification of rooms	Facility services database	Facilities services office	$0	Low Risk
University room data elements collected	Facility services database	Facilities services office	$0	Low Risk
University room data elements definitions	Facility services database	Facilities services office	$0	Low Risk
University classroom facilities	Facility services database	Facilities services office	$0	Low Risk
University laboratory facilities	Facility services database	Facilities services office	$0	Low Risk
University office facilities	Facility services database	Facilities services office	$0	Low Risk
University study facilities	Facility services database	Facilities services office	$0	Low Risk
University special use facilities	Facility services database	Facilities services office	$0	Low Risk
University general use facilities	Facility services database	Facilities services office	$0	Low Risk
University support facilities	Facility services database	Facilities services office	$0	Low Risk
University health care facilities	Facility services database	Facilities services office	$0	Low Risk
University residential facilities	Facility services database	Facilities services office	$0	Low Risk
University unclassified area	Facility services database	Facilities services office	$0	Low Risk
University unassignable area	Facility services database	Facilities services office	$0	Low Risk
University structural area	Facility services database	Facilities services office	$0	Low Risk
List of course information	Registrar database	University registrar	$1	Moderate Risk
Course instructors’ names	Registrar database	University registrar	$1	Moderate Risk
Course names	Registrar database	University registrar	$1	Moderate Risk
Course numbers	Registrar database	University registrar	$1	Moderate Risk
Course section numbers	Registrar database	University registrar	$1	Moderate Risk
Course days	Registrar database	University registrar	$1	Low Risk
Course beginning hour	Registrar database	University registrar	$1	Moderate Risk
Course ending hour	Registrar database	University registrar	$1	Moderate Risk
Course building number	Registrar database	University registrar	$1	Moderate Risk

Course room number	Registrar database	University registrar	$1	Moderate Risk
Course number of students	Registrar database	University registrar	$1	Moderate Risk
Course sequence number	Registrar database	University registrar	$1	Moderate Risk
Course record type	Registrar database	University registrar	$1	Moderate Risk
List of university graduate students	Directory database	University directory	$1	Moderate Risk
List of university undergraduate students	Directory database	University directory	$100	Moderate Risk
List of university doctoral students	Directory database	University directory	$100	Moderate Risk
List of university researchers	Directory database	University directory	$100	Moderate Risk
List of university post-doctoral	Directory database	University directory	$100	Moderate Risk
List of university research topics	Research database	Office of Research	$0	Low Risk
List of university research progress	Research database	Office of Research	$1000	High Risk
List of university research approvals	Research database	Office of Research	$5	Moderate Risk
List of university research denials	Research database	Office of Research	$5	Moderate Risk
List of university research resource allocation	Research database	Office of Research	$100	Moderate Risk
List of past university research topics	Research database	Office of Research	$5	Moderate Risk
List of past university research contributions	Research database	Office of Research	$0	Low Risk
List of past university research progress	Research database	Office of Research	$5	Moderate Risk
List of university alumni	Alumni database	Alumni office	$1	Moderate Risk
List of contributions made by university research	Research database	Office of Research	$0	Low Risk
List of contributions made by university alumni	Alumni database	Alumni office	$0	Low Risk
University awards	Alumni database	Alumni office	$0	Low Risk

List of university majors	Registrar database	University registrar	$0	Low Risk
List of university advisors	Registrar database	University registrar	$0	Low Risk
List of university scholarship applicants	Scholarship database	University scholarship office	$1	Moderate Risk
List of university approves scholarship applicants	Scholarship database	University scholarship office	$1	Moderate Risk
List of approves university scholarship amounts	Scholarship database	University scholarship office	$1	Moderate Risk
List of university athletes	Athletics database	University athletics database	$0	Low Risk
List of university sponsored sports	Athletics database	University athletics database	$0	Low Risk
List of university coaches	Athletics database	University athletics database	$0	Low Risk
List of university sports teams	Athletics database	University athletics database	$0	Low Risk
List of university sports team members	Athletics database	University athletics database	$1	Moderate Risk
University sports championships	Athletics database	University athletics database	$0	Low Risk
Notable alumni athletes	Athletics database	University athletics database	$0	Low Risk
Academic standing of athletes	Registrar database	University registrar	$5	Moderate Risk
Football team record	Athletics database	Athletics database	$0	Low Risk
Number of injuries	Athletics database	Athletics database	$5	Moderate Risk
Number of home games	Athletics database	Athletics database	$0	Low Risk
Number of away games	Athletics database	Athletics database	$0	Low Risk
Number of playoff runs	Athletics database	Athletics database	$0	Low Risk
Deepest playoff runs	Athletics database	Athletics database	$0	Low Risk
Number of years since last championship	Athletics database	Athletics database	$0	Low Risk
MVP of each year	Athletics database	Athletics database	$0	Low Risk
Longest game	Athletics database	Athletics database	$0	Low Risk

11.References

1. "Risk Classifications." Risk Classifications | University IT, uit.stanford.edu/guide/risk classifications.
2. Skowronski, Jeanine. "The Black-Market Value of Your Identity." Bankrate, Bankrate.com, 27 July 2015, www.bankrate.com/finance/credit/what-your-identity-is-worth-on-black-market.aspx.
3. "What Is Data Classification? - Definition from WhatIs.com." SearchDataManagement, searchdatamanagement.techtarget.com/definition/data-classification.
4. https://www.cmu.edu/iso/governance/guidelines/data-classification.html