Longhorn Athletics

EE361N: Information Security and Privacy

Student Name: Saptarshi Mondal

Student EID: sm72999

* ***Company selection: Your company (fictious or real, your choice) is not restricted to a Longhorn company operating on the forty acres.   The Project Description provided in the Assignment #1 offers companies with a Longhorn label as examples only and describes companies off limits.***

# Change History

|  |  |  |
| --- | --- | --- |
| Date | Description of Change | Change made by: |
| 9/11/2022 | Creation of purpose and audience description, outline data inventory and description | Saptarshi Mondal |
| 10/2/2022 | Modified the purpose and audience as well as the data inventory and added the information valuation and categorization | Saptarshi Mondal |
| 10/23/2022 | Modified the purpose and audience as well as added the Vulnerabilities and risk section | Saptarshi Mondal |
| 11/6/2022 | Modified the purpose and audience as well as added the Trusted Identity and Access Control section and fixed the errors in the vulnerabilities and risk section | Saptarshi Mondal |
| 11/20/2022 | Modified the purpose and audience as well as added the Incident Response Plan section | Saptarshi Mondal |
| 12/5/2022 | Modified the purpose and audience as well as added the Information Security and Privacy section | Saptarshi Mondal |
|  |  |  |

# Purpose (no more than one page)

 The purpose of this document is to document information security and privacy plan for Longhorn Athletics, a sports-management company which mainly acts as agents for various athletes and are the owners of various athletic venues. The content of this document consists of the audience to whom this is directed, an inventory of all the types of data used by Longhorn Athletics, along with their location and ownership. As stated earlier the document also provides the data inventory with location and ownership assignments so that it is clear where each data element is held in our systems and who is responsible for it. It also contains a categorization and valuation of all the above-mentioned information and provides the rationale for this categorization and what its estimated value will be according to sources. It also highlights the vulnerabilities and risks that the company possess which might cause this information to be threatened. It also expands by giving a classification of these vulnerabilities as well as a table about their impacts and examples. It also gives estimates for the risk for two of the risks given in the table. The document also highlights the stakeholders, the assigned access controls specifications and the assigned assurance levels for those stakeholders. The document gives information about who can be trusted with this information, the level of clearance that they have and their ability to share this information with others. The document contains a response plan of what should be done in case of an incident. Finally, the document also contains information about the companies trust framework, the principles it uses to implement the trust framework and a set of countermeasures to ensure that a breach does not happen. This content is important to the company as it gives a basic plan for the company to follow in case of a security breach and assess the damage the breach has caused. The reason that the description of the audience is provided so that it is clear to everybody exactly who should read this document The document also highlights the stakeholders, inventory, inventory location and ownership so that it is clear to everybody reading this about who owns the data of Longhorn Athletics, what is the inventory of Longhorn Athletics as well as its location and finally which entities have a stake in the data.

# Audience *(no more than a page)*

The document is for the primary users, modifiers, and owners of the data. In the case of Longhorn Athletics, the data owners refer to the Longhorn Athletics Company, a company which acts as sports agents for athletes as well as has the ownership of various stadiums and venues. The primary users and modifiers of this data include the staff of the company as well as the clients. The staff of the Longhorn Athletics also have the right to this data but to various degrees. The payroll department, Basketball department, HR department, Baseball department, Football department, Client department, IT department and the Venue department have all access to the modification and addition of data elements that they own. The higher-level staffs and executives have access to information that the company determines as being “classified” or “restricted” for the company and can only be accessed by authorized clearance. Clients and employees have the right to ask for their personal information or modify their personal information, however these modifications will cause them to be held accountable in case the information supplied is incorrect or out of data. The document is also for the various government entities that are interested in our information security and privacy processes and systems, specifically the NIST (National Institute of Standards and Technology) at the U.S. Department of Commerce or the CISA(Cybersecurity and Infrastructure Security Agency). Also, this document should be given to any cybersecurity entity of a foreign government where the company has set up either stores, databases, or headquarters. This document must also be handed to third party companies who are dealing with implementing new cybersecurity measures or want to know what practices we implemented in case of a breach. This document is also aimed for our IT as well as our cyber security departments since they oversee maintaining and protecting our data.

# Data Inventory

# Information Valuation and Categorization

**Classification:**

The classification scheme is primarily based on accessibility of data to the people. The classification scheme that we will use is public, internal, confidential and restricted. To define these categories: Public means that we can give complete access to this information to anybody, internal means that this information is only used within the company by the employees, confidential means that specific authorization is mandatory to be given access to the data and restricted means that this information is not given access to the public and most of the company under any circumstances and only select individuals can investigate it. The reason that this scheme has been selected is because of the various data elements in our inventory. There are some elements in the data inventory that we have no problem being given to the public, current standings of teams, who is most likely to win which award this season etc. This information is accessible to the public not only through our agency but through other organizations as well. Then there are other data elements for example, contracts of players which are only partially available to the public, while the finer details are restricted only to the players and their respective teams. Its good publicity for the company to allow the public to know that one of their clients has been awarded a huge contract by their teams. However, if to many specifics of the contract become public then rival teams and entities may try to botch or manipulate games to ensure that the player does not earn his rightful money. Then there is some information which is completely useless to the public but may be useful for the company and its employees. Finally, there is some information that we will never give up to anybody except selected individuals, this information can be employee address, client address, employee phone number, bank accounts etc. If this information goes public under any circumstances, then it can be used by people for ill gains and can hurt our employees, clients, and our business in a big way.

References: <https://kirkpatrickprice.com/blog/classifying-data/#:~:text=Typically%2C%20there%20are%20four%20classifications,only%2C%20confidential%2C%20and%20restricted>.

https://www.techtarget.com/searchdatamanagement/definition/data-classification

**Valuation:**

The valuation scheme that we will use is : Low, Medium, High , Priceless. The first thing to understand about the valuation scheme is that the values assigned to each data element is based on what the company perceives its value to be. Low valuation refers to data which has no real monetary value. Thus, this data if sold online to other groups might be sold for less than 10 dollars. Medium valuation refers to data which has some monetary value and if sold online might be worth between 10 – 100 dollars. High refers to data elements which if stolen from the company will have serious repercussions. These data elements might go on the black market for 100-1,000 dollars. Priceless refers to data that the company under no circumstances can afford to have stolen. This is very important and expensive data which the company estimates may go between 1,000-10,000 dollars. The reasoning behind the valuation scheme is that it is important to know how much this data is worth so that it is clear to the company how much the data is worth monetarily. Then there might be some information which is worth some amount but again in the long run is still of negligible monetary value. Then there is some information which is very expensive and should be protected and finally there is data that is too valuable to be lost and can’t be lost. If the previously mentioned data types are lost it will financially hurt the company a lot. Thus, they need to be protected at all times and at all costs.

References: <https://www.imperva.com/learn/data-security/data-classification/>

https://www.anmut.co.uk/an-introduction-to-data-valuation/

**Data Asset Summary:**

The groupings according to the data classification is as follows:

Public: 94 out of 201 elements or 46.76% of the elements

Internal:69 out of 201 elements or 34.32% of the elements

Confidential: 22 out of 201 elements or 10.94 % of the elements

Restricted: 16 out of 201 elements or 7.96% of the elements

There is also a grouping based on data valuation which is as follows:

Low: 94 out of 201 elements or 46.76% of the elements

Medium: 69 out of 201 elements or 34.32% of the elements

High: 22 out of 201 elements or 10.94 % of the elements

Priceless: 16 out of 201 elements or 7.96% of the elements

Judging from the above groupings a very visible pattern seems to emerge. Public information which can be accessed by everybody is also data that the company believes has low value and it is assigned the “Low” classification. Information that is classified as being internal is used for the internal workings of the company. Thus, if this information is stolen then the working of the company will be affected, however the information which is classified as internal is not too precious to cause massive amounts of damage. Hence the data is classified as having medium value. Data that is defined as being confidential will have serious and long-lasting repercussions that the company cannot afford. As seen from the table the data elements under confidential cannot see the light of the day as it may cause a lot of people and organizations to scrutinize it and have a massive impact on the sports. Thus, it is classified as being high value. Finally, the data classified as being restricted is data pertaining to the high-profile clients which are the athletes in this case. This data is always an attractive for hackers and thus must be always guarded. If this data is stolen not only will it destroy the company’s reputation but will have a serious effect on the athlete’s career. Thus, this data is classified as being priceless. Another trend that we see is that Public and low categories have the maximum number of elements and with the increase in exclusivity and priority, the number of elements in the other categories decreases. This is also a good sign since this means that the company must only focus on a small number of data elements to guard properly, instead of all the elements.

I think that the total value of all the data elements at maximum can be around $200,000. The minimum value that the total value of all the data elements can be is $20,000. So the range of the value of the data is between $20,000 to $200,000.

# Vulnerabilities and Risks

**Importance of identifying the Risks and Vulnerabilities**

The purpose of this document will not be complete without identifying the risk and vulnerabilities that the company faces in terms of its cyber security. The reason that it is important to identify the risks and vulnerabilities is to ensure that the company knows what its vulnerabilities it has and what its impact will be. It will also additionally provide a gateway of how the company can deal with the issues. Knowing what the company’s’ vulnerabilities are will allow the company to obtain and allocate the required resources to remove those vulnerabilities. This information is again useful for everyone under the audience category. However, those who deal with the data inventory on a regular basis or are part of the department which oversees the data inventory, and its protection must pay special attention to this section.

Understanding the risks that the company faces ensures that the company does not participate or enact in any scheme which may increase those risks. These schemes may refer to not only security policies that the company implements but general policies as well. This information is also useful for the department charged with the security and oversight of the data inventory. However this information must be especially provided to the higher ups in the company.

If the company did not have information about the risks and vulnerabilities it faces then the company would not understand or know that their data has been compromised or leaked or which policies and decisions that they implement may make it more enticing for outside forced to breach their systems.

**Vulnerability of Threat Classification**

Vulnerabilities

People/Vendor

Technology

Process/Policy

Improper Training Poor poli

Outdated Technology

Presence of Backdoor for exploitation

Installation of harmful technologies

Poor Policy making

Incorrect decision making

Improper Training

Lack of oversight

Insider theft

Third Party Vendor Theft

Extortion

Third party Vendor theft

Extortion

The classification tree is divide into three categories namely people, process/policy and outdate technology. The reason is that all the vulnerabilities can be classified as vulnerabilities created by individuals, the company or the technology used by the company to protect itself. This gives us a broader spectrum of vulnerabilities to talk about and classify.

**The Matrix of Vulnerability**

The below mentioned table is called the matrix of vulnerabilities which also constitutes of the type of vulnerability, the risk posed by said vulnerability and the risk level with regards to the Confidentiality, Integrity and Availability. The risks described in the table refer to the consequences of what would happen if the threat exploited the vulnerability. The types of Vulnerability consist of the types mentioned in the tree above as well as some more. The risk level is dependent on what the company feels and is different for each of the three categories(CIA).

|  |  |  |  |
| --- | --- | --- | --- |
| ***Type of Vulnerability*** | ***Description of specific***  ***vulnerability occurrence***  ***(how the threat exploited***  ***a vulnerability)*** | ***Risk posed by vulnerability (impact caused by threat when***  ***vulnerability exploited)*** | ***Risk Level***  ***(high, medium, low)*** |
| In Insider theft | Somebody who works  or worked for the  company sold the data | Confidentiality-  All the information  which the company  would like to remain  private will be available  for everyone to buy | High Risk in terms of  Confidentiality  Integrity- There is not  Much risk in terms of  Integrity  Availability- There is not  Much risk in terms of  Availability |
| Third party Vendor  theft | A third-party company  with which the  company  may have worked with  might sell the data | Confidentiality- The  Third party company  Can use and abuse the  Data that they are  likely  To sell | High Risk in terms of  Confidentiality  Integrity- There is not  Much risk in terms of  Integrity  Availability- There is not  Much risk in terms of  Availability |
| Improper Training | The employees may  Open emails which may  Contain virus which is  Used to breach the  system | Confidentiality- The  Virus can gain access to  Information which is  Extremely sensitive  Integrity- The virus can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Improper Training | Employees leave their  Systems online and idle  Allowing a potential  Hacker to get in | Confidentiality- The  hackers can gain access  to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Presence of backdoors  for exploitation | The company makes a  Decision to implement  Certain software  Attributes which make  It easy for hackers to  Take advantage of | Confidentiality- The  hacker can gain access to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Incorrect  decision-making | The higher ups of the  Company do not  perform  The correct steps in  For security  Protection and in turn  Invite hackers to attack | Confidentiality- The  hacker can gain  access to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Outdated Technology | The company relies on  Decade old technology  To protect them making  Them easy target for  hacker | Confidentiality- The  hacker can gain  access to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Presence of backdoors  for exploitation | There is a potential  Backdoor in the security  System created by the  Company which the  Company is not aware  Of but can take  Advantage of | Confidentiality- The  hacker can gain access to  Information which is  Extremely sensitive  Integrity- The hacker can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Insider theft | Physical copies of the  Data may be stolen from  The companies premise | Confidentiality- The data  Is now available to the  Highest bidder | High Risk in terms of  Confidentiality  Integrity- There is not  Much risk in terms of  Integrity  Availability- There is not  Much risk in terms of  Availability |
| Improper Training | Employees may  Accidentally make all the  Data public giving hackers  Free rein over them for  Considerable time | Confidentiality- The  hacker can gain access to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Insider theft | Individuals from the  Company may leak the  Data to the public | Confidentiality- The data  Is now available to the  public | High Risk in terms of  Confidentiality  Integrity- There is not  Much risk in terms of  Integrity  Availability- There is not  Much risk in terms of  Availability |
| Third party Vendor  theft | A third-party vendor  May hold to the  Company’s data and  Refuse to give it up | Confidentiality- The data  Is now available to an  Unknown third party  With unknown intentions | High Risk in terms of  Confidentiality  Integrity- There is not  Much risk in terms of  Integrity  Availability- There is not  Much risk in terms of  Availability |
| Improper Training | The employees may be  Fooled by scam calls  Which may persuade  Them to give up the  information | Confidentiality-The data  Is now available for  Scammers to do so as  They please | High Risk in terms of  Confidentiality  Integrity- There is not  Much risk in terms of  Integrity  Availability- There is not  Much risk in terms of  Availability |
| Incorrect  decision-making | Hackers may use the  Data that the company  Has deemed as being  Of low risk to gain  Access | Confidentiality- The  hacker can gain access to  Information which is  Extremely sensitive  Integrity- The hacker can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Installation of harmful  technology | The company may have  Installed malwares them  Selves under the guise  That they are software’s  Used by the company | Confidentiality- The  hacker can gain access to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Third party  Vendor theft | Company may be under  Attack by another  Company using hackers  And public information | Confidentiality- The  hacker can gain access to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Third party  Vendor theft | Company may be  attacked  By governments or  Interest groups  Who may have planted  Various malware in the  system | Confidentiality- The  Groups can gain  access to  Information which is  Extremely sensitive | High Risk in terms of  Confidentiality  Low Risk in terms of  Integrity  Low Risk in terms of  Availability |
| Extortion | The higher ups  computer  May be hacked and  used  To access the information | Confidentiality- The  hacker can gain access  to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Extortion | The hackers may hack  The information security  Or IT departments to  Obtain the information  From them | Confidentiality- The  hacker can gain  access to  Information which is  Extremely sensitive  Integrity- The hacker  can  Also manipulate the  Data in the company  Database for nefarious  Purpose  Availability-Might not  Allow employees access  To the data in the right  Time in the right format | High Risk in terms of  Confidentiality  High Risk in terms of  Integrity  High Risk in terms of  Availability |
| Extortion | Employees may be  Physically forced or  Blackmailed to give up  The information | Confidentiality-The data  Is now available for  Scammers to do so as  They please | High Risk in terms of  Confidentiality  Integrity- There is not  Much risk in terms of  Integrity  Availability- There is not  Much risk in terms of  Availability |

**The risk estimates**

1)Risk estimate in case of third party vendor theft(A third party company refuses to give up the data)

According to an articles regarding a similar case(<https://www.texastribune.org/2014/05/09/texas-sues-xerox-recover-millions-misspent-money/> and https://www.texasattorneygeneral.gov/news/releases/ag-paxton-recovers-record-236-million-texas-medicaid-fraud-settlement) The company could take the third party to the court and win over 200 million dollars in settlement. Since cases as this take a lot of time and money, it is reasonable to state that the lawyers may charge over 60 million dollars as payment. Also notifying the victims may also take roughly 2 million dollars. In terms of reputation damage it can make the company seem as being too trustworthy of others and weak in certain cases and make the leagues less interested in doing business with the company. Most of the individuals may also be keen to leave the company as they believe that their data can be easily stolen, showcasing the reputational damage to the company and the emotional damage sustained by the individuals. The company may be forced to make bargains which could end up costing a lot of the companies profit in the future to convince shareholders and athletes to not bail.

2)Risk estimate in case of accidentally making data public:

In such a case considerable amount of time and money may be spent in trying to figure out who may have accessed the data . This endeavor itself may take the company years. Taking the information from this article(<https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/>), it may cost the company less than 10 million dollars(conservatively it may be around 2 to 3 million dollars) and a lot of time to figure out who may have accessed their data. Then the company may agin be forced to notify victims and pay them some amount which could total to 1-2 million dollars. The company’s reputation may take a significant hit and have a negative impact on business and cause unnecessary emotional distress to the individuals who have given their data to us.

# Trusted Identity for Information Access and Sharing Controls

## Access Control Design

The access control that the company will be using is an Attribute based access control. In this access control the parameters for the role will be the role, the department, employee id and registered device. Just to clarify the role, which is the title of the job that the employee holds will provide the subject/user attributes, the department will provide the environment attributes and the employee id will provide the information attributes.

The rationale for selecting such an access control system is that the company consists of too many departments which have different sort of data that they work with. Thus, it is imperative to know, which department the user belongs to so that they can access information useful for their department instead of being handed information which they have no use for. The department also acts as an approval agent ensuring that there is some sort of identification done by people instead of systems especially when dealing with external stakeholders. Going further into this situation, the company also realizes that some of the information which each department deals with is too sensitive to be allowed complete access to even the entire department, thus title or role is asked to ensure that only certain individuals who have the required clearance have access to the most sensitive information of their department. Finally, all this is encapsulated under the fact that only valid employees who work for the company have access to any of the information that the company holds, so employee id is required to meet this requirement. In case of external stakeholders, the employee id and registered device acts as a verification that they are who they say they are.

## Stakeholder types requiring access

|  |  |
| --- | --- |
| **Type of Stakeholder** | **Description of the Stakeholder (include the activities this stakeholder may perform requiring their information access and authorizations)** |
| **Auditing firms** | **This is an external stakeholder who is hired by the company to advice the company on how to decrease inefficiencies, reduce costs, and otherwise achieve organizational objectives. Due to this reason, they make require seeing information including but not limited to our payroll, IT and Venue department. Thus, they will require the appropriate information access and authorizations** |
| **Clients** | **This is an external stake holder. They must be given access to information pertaining to only them so that they can modify their personal information or add their personal information.** |
| **The governments tax department** | **This is an external stakeholder who may ask for information about our profits, revenues, budgets, and other financial decisions.** |
| **CEO, CFO, and shareholders** | **This is an internal stake holder. They may ask for any of the information stated above and also any additional information such as an employees id , salaries etc.** |
| **Employees** | **This is an internal stake holder. These stakeholders are primarily concerned with the addition, modification, or usage of data. Thus, they require access to the data and the appropriate authorizations** |

## Level of Assurance for Stakeholder Authentication

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Type of Stakeholder** | **Classification for Information Accessed (see Section 5)** | **IAL**  **(Level 1, 2 or 3)** | **TAL**  **(Level 1, 2, 3, or 4)** | **LOA**  **(Levels 1-4)** | **Justification for Assignment of Assurance Levels** |
| **Auditing Firm** | **Confidential/Internal** | **2** | **2** | **2** | **This stakeholder works with data that is of moderate to near high importance for the company, thus moderate levels of assurance are selected** |
| **Clients** | **Public/Restricted/Confidential** | **3** | **4** | **4** | **This stakeholder directly works with the most prized and important data of the company, thus the IAL,TAL and LOA need to be set to the maximum to ensure that only the authorized personnel gets access to the data** |
| **The governments tax department** | **Confidential/Internal** | **1** | **1** | **1** | **The stakeholders works with data that is similar to what is used by a stakeholder mentioned above. However this is a government body and thus according to the company can be trusted a lot more than the previously mentioned stakeholder. Thus it is assigned lower levels of assurance than the levels assigned to the previous stakeholder** |
| **CEO, CFO and shareholders** | **Public/Restricted/Confidential/Internal** | **3** | **4** | **4** | **This stakeholder has the authority to get the most prized and important data of the company, thus the IAL,TAL and LOA need to be set to the maximum to ensure that only the authorized personnel gets access to the data** |
| **Employees** | **Public/Confidential/Internal** | **2** | **3** | **3** | **This stakeholder has access to data that is not the most important data of the company but just falls below that category does it requires the second highest assurance levels** |

## Stakeholder access control

*Define the control specifications required for automated, electronic access decisions. These control specifications must be described for each stakeholder type. Remember, a programmer must code this specification for automated access control and the answer/result from the access control decision is “Yes” or “No.”*

|  |  |  |
| --- | --- | --- |
| **Type of Stakeholder** | **Access Control Specification** | **Access Control Specification applies to what part of the Information Inventory.** |
| Auditing Firm | The auditing firm has access to all the financial records present in the venue and IT department | Internal |
| Auditing Firm | The auditing Firm must also provide an employee id to get the financial records in the payroll department | Confidential |
| Clients | The Client must provide their employee id and can only access the information on the Client department from their registered device after getting approval from the Client department | Restricted |
| The government tax department | The government tax department has access to the financial records present in the venue and IT department | Internal |
| CEO, CFO and shareholders | CEO, CFO and shareholders must provide their respective employee id and can only access information from their registered device after getting approval from the Client department | Restricted |
| Employees | Employees can only access information pertaining to their department from their registered device after providing their employee id | Confidential |
| Clients | The Client must provide their employee id and can only access the information on the Client department from their registered device. | Confidential |
| Clients | The Client must provide their employee id and to access the information. | Public |
| The government tax department | The government tax department has access to these financial records present in the venue and IT department. | Confidential |
| CEO, CFO and shareholders | CEO, CFO and shareholders must provide their respective employee id and can only access information from their registered device. | Confidential |
| CEO, CFO and shareholders | CEO, CFO and shareholders must provide their respective employee id to access information | Internal |
| CEO, CFO and shareholders | CEO, CFO and shareholders must have access to the information | Public |
| Employees | Employees can only access information pertaining to their department after providing their employee id | Internal |
| Employees | Employees can only access information pertaining to their department | Public |

# Incident Response Plan (ASSIGNMENT #3)

## Incident Identification

|  |  |  |  |
| --- | --- | --- | --- |
| 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?) |
| Virus | Employee states their computer is not working properly and they cannot access some files | At this stage it is not clear exactly what the problem is and therefore what the loss could be. It is only after further research by the IT department to identify why the computer is not working can we verify what losses are we looking at. | Currently all the departments except the affected departments computers can work freely with no problems whatsoever, |
| Ransomware | A staff person reports their files cannot be opened and they have a notice on their screen. | At this stage it is we have to figure out what the notice says. This means that the IT department must understand the demands before we can calculate the losses the company faces. However, the situation does not look good, and the company must expect that heavy loss in data, finance and time is coming in the future. | Currently all the departments except the affected departments computers can work freely with no problems whatsoever, |
| Compromised web site | Staff reports that the web site’s content has been changed to something obscene. | At this stage this is not really a problem in terms of data or finance or time. However, having an obscene web site will be extremely damaging to the company’s reputation, so it must be fixed as soon as possible | Currently all the departments except the affected departments computers can work freely with no problems whatsoever/ The Client department may have to work overtime to fix any PR issues. |
| Slow Server | Staff reports the file server is running very slow. | This need not be anything serious. However, the IT department must check why the problem is taking place. Now losses cannot be calculated. | Currently all the departments except the affected departments computers can work freely with no problems whatsoever, |
| Phishing | A suspicious email is sent to an employee asking for data about the company. | It is more important to figure out who sent the email. According to the situation no data has been shared with sender, so there seems to be no loss in that sense. However, some amount of time and money may be spend to figure out the identity of the scammers. | Currently all the departments except the affected departments computers can work freely with no problems whatsoever, |

|  |  |  |  |
| --- | --- | --- | --- |
| 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?) |
| Virus | Employee states their computer is not working properly and they cannot access some files and IT department finds a virus on that system. | The company knows that there is a virus in the system. At this moment we however do not know if the most sensitive data has been lost or not. All the other sets of data should be assumed as being compromised. There will a substantial amount of time and money needed to remove the virus from the system, built a new security system, attach new measures and figure out who might be responsible for the attack. Their will also be some damage to the reputation of the company after the attack. | Only departments who work with ‘Low’ valuation of data may be allowed to work without interruptions. |
| Ransomware | A staff person reports their files cannot be opened and they have a notice on their screen. A Ransomware virus is on the user’s computer and has a notification that files are encrypted and bitcoin payment is required to decrypt | According to the situation, it is more probable that the attackers were more interested in preventing the company from accessing the data then stealing the data. Thus the data can be deemed as not being compromised. However, the company will have to finance a new security system, counter measures and pay the ransom all of which will require a substantial finance resource and some time. However, if both the parties keep quite it can be possible that the reputation of the company is intact. | All departments which have access to the system can still work, however it is best to stick with the data which are considered as being ‘Low’ or ‘Medium’ in valuation. |
| Compromised web site | Staff reports that the web site’s content has been changed to something obscene. The IT department notices files have been changed on the web server | The company knows that in this case some data has been modified, but it is not clear if the most sensitive data is out of company control. The company will have to rebuild the website along with server, security systems and the counter measures which will require a substantial amount of funds and time. A obscene web site will cause a serious hit to the company’s reputation | Only departments working with ‘Low’ valuation data might be allowed to continue work. The Client department may have to work overtime to fix any PR issues |
| Slow Server | Staff reports the file server is running very slow. The IT department notices a rogue active network port scan | This could very well mean that the attackers were looking for open doors to the data. At best case they got access to none of the data. At worst case, they found some of the data. However, it is not clear if the most sensitive data has been lost or not. Substantial amount of money and time will be used to patch the holes, find any other open points, revamp and upgrade the security of the servers and recoup any loses due to data. It is possible to keep this inhouse and maintain the company’s reputation. | Most departments not part of the affected computer and the connected servers may be free to work. However it is recommended that they stay away from the usage of ‘Medium’, ‘High’ or ‘Priceless’ valuation data elements. |
| Phishing email | Employee opens a phishing email and may have shared confidential information. | There is loss of confidential data, but this is not the most sensitive data that the company holds. There is not real lose in reputation as this can be kept in house. Certain amount of money and time will be spent trying to retrieve the data as well as figure out who sent the email. | All computers who did not receive the email may work freely. Aside from the server whose data was shared all other servers can be used without any problems. |

|  |  |  |  |
| --- | --- | --- | --- |
| 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?) |
| Virus | Employee states their computer is not working properly and they cannot access some files and IT department finds a virus on that system. The virus has given control to the hacker and restricted data has been accessed. | The company knows that there is a virus in the system and all the data including the most sensitive data has been lost. There will a massive amount of time and money needed to remove the virus from the system, built a new security system, buy and built new servers, attach new measures and figure out who might be responsible for the attack. There will also be a lot of damage to the reputation of the company after the attack. | None of the departments will be allowed to do any work whatsoever. |
| Ransomware | A staff person reports their files cannot be opened and they have a notice on their screen. A Ransomware virus is on the user’s computer and has a notification that files are encrypted and bitcoin payment is required to decrypt. Restricted data on file servers were encrypted by the Ransomware and the hackers have them on their own servers | All the data must be deemed as compromised. The company will have to finance a new security system, counter measures, new servers, figure out who was responsible for the attacks, how did this happen in the first place and pay the ransom all of which will require a substantial finance resource and some time. However, if both the parties keep quite it can be possible that the reputation of the company is intact. | None of the departments will be allowed to do any work whatsoever. |
| Compromised web site | The IT department sees that the server has been compromised and is hosting an illegitimate, obscene web site and institutional data has been accessed. | The most sensitive data is out of company control. The company will have to rebuild the website along with server, security systems, figure out who was behind it, how it took place and why it was done and the counter measures which will require a huge amount of funds and time. An illegitimate and obscene web site will cause a serious hit to the company’s reputation resulting in decline in stock values, bad press as well as several investor and board meetings | None of the departments will be allowed to do any work whatsoever. The Client department may have to work overtime to fix any PR issues |
| Slow Server | Staff reports the file server is running very slow. The IT department notices a rogue active network port scan. That employee’s compromised computer has restricted data on their computer. | The most sensitive data has been lost or not. Huge amount of money and time will be used to patch the holes, find any other open points, buy new servers , built these servers ,revamp, and upgrade the security of the servers and recoup any loses due to data. There will be a major hit on the company’s reputation as the most sensitive data of the company has been stolen. | None of the departments will be allowed to do any work whatsoever. |
| Phishing email | Employee opens a phishing email and has shared confidential and restricted information. | The most sensitive data that the company holds is lost. There is not real lose in reputation as this can be kept in house. Huge amount of money and time will be spent trying to retrieve the data as well as figure out who sent the email as well as implementing new security measures such as a bot which checks for such mails in the first place and deletes them right before they are read. | None of the departments will be allowed to do any work whatsoever. |

## Incident Prioritization

|  |  |  |  |
| --- | --- | --- | --- |
| **Incident Priority Level** | **\*Criteria. Each criteria 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 (Information Impact = None) AND Recoverability = (Regular) | The level 1 is the least severe of all incident priorities. Thus the functional impact needs to be set to minimum, which in this case is None. Similarly the Information Impact and Recoverability need to be set to the least severe levels which are None and Regular respectively. In this case there is no functional and information impact on the company and the company can recover the data in a finite amount of time with existing resources | Somebody stole the public data from the company. This data is readily available making it easily recoverable and at the same time is not sensitive data in any situation, meaning it has no functional and information impact. |
| **Level 2** | (Functional Impact = Low) AND (Information Impact = Proprietary Breach ) AND Recoverability = (Supplemented) | Level 2 is a bit more severe than level 1. Thus, the functional impact is decided to be low and the information impact is set to Proprietary Breach. Recoverability is set to Supplemented. Again as this is a bit more severe than level 1, the functional and Recoverability levels are set at a level higher than their counterparts in level 1, to indicate that they have a bit more effect on the companies functionality (but are still low) and require a bit more effort to recover (but still easy) in finite amount of time. Proprietary Breach refers to unclassified proprietary information which will be important for the company is not as sensitive. | Hackers steal the internal data from the company. This data is more important than the public data and will have a bit more impact on the functioning of the company, as they may be used the competitors. This data is also still present in the database and after verification and cross validation, which will require some additional resources, can be used by the company again. |
| **Level 3** | (Functional Impact = MEDIUM) AND (Information Impact = Proprietary Breach AND Integrity Loss) AND Recoverability = (Extended) | Level 3 is more severe than Level 2. Thus the functional impact is set to medium, information impact is set to Privacy Breach and Recoverability is set to Extended. Medium functional impact indicates a much higher effect on the working of the company than the impact felt on level 2 and the company may lost the access to some critical services. This is again fits with level 3’s criteria of being more severe than level 2. Proprietary Breach was explained in the previous level but this coupled with the fact that the information on the database has also been modified as indicated by Integrity loss. This magnifies the information impact. The Recoverability is set to extended because considering that there is proprietary breach and integrity loss, a lot more time and resources will be required to get the data back . | Hackers steal the internal data of the company and completely corrupt the integrity of the internal data stored in the company’s databases. This has a greater effect on the functioning of the company as well as on its information database. Similarly as the integrity of the database has been lost more work will need to be done to recover the lost data. This is mainly through recollection of the data through the original sources. |
| **Level 4** | (Functional Impact = HIGH) AND (Information Impact = PrivacyBreach AND IntegrityLoss) AND Recoverability = (Not Recoverable) | Level 4 is nearly as high as Level 5 and more severe than level 3. Thus the functional impact is set to high to indicate the rise in severity in comparison to level 3 and its near status to level 5. The company has lost access to most of its critical services, which fits the justification of level 4. Information impact is a combination of privacy breach and integrity loss, this is because again level 4 is very severe cases and since privacy breach deals with the loss of sensitive information and integrity loss is that the sensitive information has been modified or deleted, this is seen as a justified information impact for this level. Since the information impact is so severe, it is more likely that this data will not be feasible recoverable and will require launch of investigation. Again, this fits with the general justification of level 4 | The company’s restricted and confidential data is stolen and deleted from the databases. Again this affects most of the daily working of the company and is not recoverable at all. |
| **Level 5** | (Functional Impact = HIGH) AND (Information Impact = PrivacyBreach AND  ProprietaryBreach AND IntegrityLoss) AND Recoverability = (Not Recoverable) | Level 5 is the most severe case. While the functional impact and recoverability criteria is like level 4, it has an additional factor in information impact in the sense that there is loss of sensitive and proprietary data as well as modification of such data in the databases. This makes it a bit more severe than level 4. | The hackers steal internal, confidential and restricted data while modifying the databases containing data elements of this data classification. Again this completely stops the working of the company and will not be recoverable at all. |

## Incident Response Team

|  |  |
| --- | --- |
| **Incident Response Team Member Role** | **Incident Response Team Member Responsibility** |
| Team Leader | Coordinates the overall direction and strategy of response activities and ensures the team stays focused on minimizing damage, recovering quickly, and operating efficiently. |
| Investigator | Coordinates efforts to determine an incident's root cause. It's important to gather as much relevant information as possible. Specifically, information that can provide value to correct the acute issue as well as prevent future issues. |
| Lead Communications Director | Manages relevant [internal and external communications](https://www.techtarget.com/searchsecurity/tip/Incident-response-How-to-implement-a-communication-plan) necessary for the incident response. Communications may be required across an organization's teams and departments, or with external stakeholders. |
| Documents Keeper | Keeps records of incident response measures and activities. |
| Legal Counsel | Ensures that the incident response activities taken line up with laws and regulations to protect the organization. |

## 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** | IT department | Filing a request form on the employee portal or sending an email to the department | Within 5 minutes of discovery |
| **Level 2** | Investigator | Sending an email from the IT department’s email address to the Investigator | Within 10-50 minutes of discovery |
| **Level 3** | Incident Response Team | The investigator sends the request for his team’s involvement through direct phone call to the Team leader who then requests their assembly at the location to get a clear picture of the problem | Within 1-3 hours of discovery |
| **Level 4** | CEO, | The team leader sends a direct phone call to the CEO to let them know about the seriousness of the problem | Within 4-8 hours of discovery |
| **Level 5** | Shareholders and Board of Directors | The CEO holds and emergency meeting to notify the major shareholders and board of directors that there has been a breach and their current efforts to contain it | A day of discovery |

# Information Security and Privacy: Trust Frameworks, Technology and Design Principles (ASSIGNMENT #4)

## Trust Framework

The trust framework that I have selected is the Isolated Model Trust Framework*.* This framework was discussed in the class. The framework basically forces a user to have multiple authentication credential to get access to the different service provider entities. The main problem with this model is user convenience, as the user has to remember multiple different authentication credentials for different service entities. But in terms of complexity, data security or implementation, it is as good as any other framework. The rationale behind choosing this framework is simple. All the departments are more or less operate in a separate space from each other. Isolated Model just follows the framework the architecture already in place. All other frameworks may be better of in terms of user convenience, but the main problem is that one credential can be used for all other service providers, which this company wants to avoid. The company does not see any reason why the Client departments credential can be used to access the Venue department’s servers. This framework prevents employees from accessing data which is not of their department. It also makes it difficult for hackers or scammers to just try to take the credentials of any employee to access all the servers. Thus the Isolated Model Trust Framework is best suited for the company’s needs.

## Select Technology Solutions for your selected Trust Framework

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Data Classification** | **Technology or Design Principle** | **CIA Protection?** | **Rationale for selection of Technology and/or Method** |
| **Data at Rest** | Internal  Confidential, Restricted | File Encryption | Confidentiality,  Integrity | This is the most general protection technology that the company can implement on a regular day to day basis to make sure that no unauthorized personnel can access or modify this information. It is relatively the cheapest protection the company can obtain and also the easiest to implement via use of encryption software. |
|  | Confidential and Restricted | Data Leak Prevention software | Availability | This technology has the reputation of being able to prevent any potential breach events by proactively checking the contents of requests as well as incoming and outgoing traffic. This in turn ensures that the employees who work with this sensitive data can have uninterrupted and timely access to this data without any problems. |
|  | Confidential, Restricted | Database Encryption | Confidentiality, Integrity | This is the most secure form of protecting the information because it uses the most primitive concept-instead of encrypting individual files, the databases which contain these types of data are completely encrypted ensuring that no one can access this information at any point of time. It is also convenient for the company as most of the sensitive data of the company is restricted to a few databases. |
|  | Internal | Digital rights management Software | Availability | This technology allows only certain rights such as reading or editing without giving complete access to the data. This is convenient for data which is important for the company but is not highly valuable and is used for day-to-day basis. It is also very useful as it ensures that the employees can have uninterrupted and timely access to the data without any issues. |
| **Data in Transit** | Internal  Confidential, Restricted | Email Encryption | Confidentiality, Integrity | This technology is the most basic protection the company can offer during data in transit. It is most easily implemented and are common tools for day to day use. |
|  | Confidential, Restricted | https | Confidentiality, Integrity | This technology is used on a regular basis across all of internet to exchange information. This technology operates at the highest layer of the [TCP/IP model](https://en.wikipedia.org/wiki/TCP/IP_model) and has a reputation of being extremely secure. It is also well known for being able to stop man-in-the middle attacks as well as prevent eavesdropping and tampering. This technology is so secure that hackers can at best know that there is a connection and transfer of data between two machines. It is perfect for the most sensitive data in the company |
|  | Internal | Managed File Transfer | Availability | This technology works by uploading the data onto a platform and then sending a secure hyperlink which is password accessed or has an expiration date. This provides reasonable protection against hardware failures and ensures that employees have uninterrupted access to the data. |
|  | Restricted, Confidential | CASB | Availability | This is technology that can be used by the company by putting all the data on the cloud. It is also easier to transmit data across different entities using the cloud. The CASB technology works similar to Data Loss Prevention technology, in the sense that it allows authorized personnel to have uninterrupted access to the sensitive data even when its being transmitted. |
| **Access to Data** | Confidential, Restricted | Principle of Separation of Privilege | Confidentiality, Integrity | This principle states that the system should not grant access based on a single factor. This principle must be implemented for the most sensitive data in the company. Having only one factor be responsible for allowing access and modification of this highly sensitive data is too risky as a practice. Thus multiple factors need to be met before such data can be accessed or modified. |
|  | Internal  Confidential, Restricted | Principle of Complete Mediation | Confidentiality, Integrity | This data principles states in general all access must be checked. Again, this is a very basic principle that must be implemented throughout the system to ensure that no unauthorized access or modification to data takes place. |
|  | Restricted, Confidential | Principle of Fail-Safe Defaults | Availability | This practice states that unless explicit access to the data is given, the system must deny access to the data. This ensures that authorized people have continuous uninterrupted access to the data without any problems whatsoever. |
|  | Internal  Confidential, Restricted | Principle of Least Common Mechanism | Availability | This principle basically asks that sharing mechanism be prevented. This is helpful because if there are no sharing mechanisms, the authorized personnel can have uninterrupted access to data without having any delays or time constraints. |

## Solution Set for Network and Web Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Solution** | **Solution Description** | **These Solutions will prevent or reduce risks** | **Does the Solution improve Confidentiality? Integrity? Availability? Authenticity?** | **These Solutions may (in most instances should) enable the Company’s ability to comply with the following laws and regulations? Name Law or Regulation and describe how** |
| Firewall | [Firewalls](https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/) control incoming and outgoing traffic on networks, with predetermined security rules. Firewalls keep out unfriendly traffic and is a necessary part of daily computing. | Prevent malware and application layer attacks and prevent unauthorized access and collection | Confidentiality, Integrity | COPPA,GDPR  This l technology ensures that there is no unauthorized access to information or collection pertaining to children and EU citizens |
| Network Segmentation | defines boundaries between network segments where assets within the group have a common function, risk or role within an organization | Prevents unauthorized access to data and ensures that certain individuals have complete | Availability |  |
| Zero Trust Network Access | The zero trust security model states that a user should only have the access and permissions that they require to fulfill their role. | Prevents unauthorized access to data | Authenticity, Confidentiality |  |
| Website Monitoring Service (LogicMonitor) | designed to monitor and ensure uninterrupted site access and minimize downtime. It also optimizes site performance and helps in keeping the website online and running constantly. | Prevents unauthorized access or modifications to data and prevent downtimes | Availability, Confidentiality Integrity |  |
| Two factor authentication (Duo) | When user tries to access servers, they are required to give two factors to confirm that they are who they say they are | Prevents unauthorized and unauthentic access to information | Confidentiality, Authenticity |  |
| Global Content Delivery Network | A content delivery network (CDN) refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content.  A CDN allows for the quick transfer of assets needed for loading Internet content including HTML pages, JavaScript files, stylesheets, images, and videos. | Prevents long times for access to data as well as downtimes | Availability |  |
| Sandboxing | cybersecurity practice where you run code or open files in a safe, isolated environment on a host machine that mimics end-user operating environments. | Ensures that there is no modification to the files such as change in data or even hidden viruses | Integrity |  |
|  |  |  |  |  |

# **Appendix A: Enterprise Information**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Serial Number | Data Element | Location | Owner | Valuation | Classification |
|  | Employee Name | HR servers | HR department | Low($0-$10) | Public |
|  | Employee phone number | HR servers | HR department | Low($0-$10) | Public |
|  | Employee id | HR servers | HR department | Medium($10-$100) | Internal |
|  | Employee email id (work) | HR servers | HR department | Low($0-$10) | Public |
|  | Employee email id  (personal) | HR servers | HR department | High($100-$1,000) | Internal |
|  | SSN of employees | HR servers/Payroll servers | HR department/Payroll department | High($100-$1,000) | Confidential |
|  | Employee address | HR servers/payroll servers | HR department/Payroll department | High($100-$1,000) | Confidential |
|  | Employee W-4 form | payroll servers | Payroll department | High($100-$1,000) | Confidential |
|  | Employee laptops | HR servers | HR department | High($100-$1,000) | Confidential |
|  | Number of offices in the country | HR servers | HR department | Low($0-$10) | Public |
|  | Number of employees in the country | HR servers | HR department | Low($0-$10) | Public |
|  | Other Withholding forms | Payroll servers | Payroll department | High($100-$1,000) | Confidential |
|  | Benefits and deductions | Payroll servers | Payroll department | High($100-$1,000) | Confidential |
|  | Hours worked | Payroll servers | Payroll department | High($100-$1,000) | Confidential |
|  | Time off | Payroll servers | Payroll department | High($100-$1,000) | Confidential |
|  | Gross wage | Payroll servers | Payroll department | High($100-$1,000) | Confidential |
|  | Pay rate | Payroll servers | Payroll department | High($100-$1,000) | Confidential |
|  | Names of clients | Client department’s server | Client department | Low($0-$10) | Public |
|  | client’s phone number | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | client’s special id in the system | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | client’s email id (work) | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | client’s email id (personal) | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | client’s address | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Clients’ current health condition | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s health history | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s training regimen | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Clients eating regimen | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s daily schedule | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s net worth | Client department’s servers | Client department | Low($0-$10) | Public |
|  | Client’s yearly salary | Client department’s servers | Client department | Low($0-$10) | Public |
|  | Clients’ sponsorship deals | Client department’s servers | Client department | Low($0-$10) | Public |
|  | Charities and organizations represented by client | Client department’s servers | Client department | High($100-$1,000) | Confidential |
|  | Clients current contract | Client department’s servers | Client department | Low($0-$10) | Public |
|  | Client’s SSN | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s bank account(checking) | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s bank name | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s banks routing number | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s list of personal contacts | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Client’s immigration status | Client department’s servers | Client department | Priceless($1,000-$10,000) | Restricted |
|  | Football clients passing yards | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients rushing yards | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients receives | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients forced fumbles | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients tackles combo | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients interceptions | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients fields goals made | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients kickoffs | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients kickoff returns average | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients punting average | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients punting returns average | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients passing attempts | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients completion | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients rushing attempts | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients rushing touchdown | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients receiving yards | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients receiving touchdowns | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients fumble recovery | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients fumble recovery touchdown | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients assisted tackles | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients solo tackles | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients intercepted touchdowns | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients intercepted yards | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients field goals attempted | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients longest field goal made | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients kickoff yards | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football client’s kickoff return yards | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients kickoff return | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients kickoff return touchdown | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients punting net average | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients punting net yards | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients punting returns | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Football clients punting return touchdown | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Schedule of football season | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Current standings of football teams | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Odds of each team to win Super Bowl this year | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Odds of each team to win the conference championship this year | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the MVP award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the OPOY award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the DPOY award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the ROTY award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the CPOTY award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the Super Bowl MVP award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the Pro Bowl | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the All Pro team | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the All Rookie team | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the Butkus award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Current ranking of football players for the Deacon Jones award | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Basketball clients game played | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients field goal percentage | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients 3-point percentage | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients 2-point percentage | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients effective field goal percentage | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients free throw percentage | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients total rebounds per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients assists per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients steals per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients blocks per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients turnovers per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients personal fouls per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients points per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Basketball clients minutes played per game | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Schedule of basketball season | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Current standings of basketball teams | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Odds of each team to win NBA finals this year | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Odds of each team to win NBA Conference finals this year | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Odds of each team to make the playoffs | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win DPOY award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win Conference finals MVP award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win MIP award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win MVP award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win ROTY award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win DPOY award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win SMOTY award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to win Finals MVP award | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All star team as starters | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All-star team as the bench | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All-NBA first team | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All-NBA second team | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All-Defensive first team | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All-Defensive second team | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All-Rookie first team | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Current ranking of basketball players to make the All-Rookie second team | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Baseball clients at base number | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients runs | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients hits | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients doubles | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients triples | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients homeruns | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients average | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients on base percentage | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients slugging percentage | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients strikeouts | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients earned run average | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients shutouts | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients saves | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients innings pitched | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients hit batsmen | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients walks and hits per innings pitched | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients batting average against | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Baseball clients stolen base | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Schedule of basketball season | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Current standings of baseball teams | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Odds of baseball teams to win Commission trophy | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Odds of baseball teams to win Warren C Giles trophy | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Odds of baseball teams to win William Harridge trophy | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win MVP award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win Cy Young award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win ROTY award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to make the All-MLB first team | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to make the All-MLB second team | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the Golden Glove award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the Silver Slugger award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the Hank Aaron award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the CPOTY award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the World Series MVP | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the League Championship Series MVP | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the All-Star Game MVP | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the Reliever of the Year award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Ranking of baseball players to win the Edgar Martinez award | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Upcoming free agency dates for football | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Upcoming free agency dates for basketball | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Upcoming free agency dates for baseball | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Upcoming free agency catches for football | Football department’s servers | Football department | Low($0-$10) | Internal |
|  | Upcoming free agency catches for basketball | Basketball department’s servers | Basketball department | Low($0-$10) | Internal |
|  | Upcoming free agency catches for baseball | Baseball department’s servers | Baseball department | Low($0-$10) | Internal |
|  | Upcoming draft dates for football | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Upcoming draft dates for basketball | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Upcoming draft dates for baseball | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Current ranking of high school players across the country for football | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Current ranking of high school players across the country for basketball | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Current ranking of high school players across the country for baseball | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Current ranking of university players across the country for football | Football department’s servers | Football department | Low($0-$10) | Public |
|  | Current ranking of university players across the country for basketball | Basketball department’s servers | Basketball department | Low($0-$10) | Public |
|  | Current ranking of university players across the country for baseball | Baseball department’s servers | Baseball department | Low($0-$10) | Public |
|  | Projected draft rankings for football | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Projected draft rankings for basketball | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Projected draft rankings for baseball | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Overseas players to keep an eye for in football | Football department’s servers | Football department | Medium($10-$100) | Internal |
|  | Overseas players to keep an eye for in basketball | Basketball department’s servers | Basketball department | Medium($10-$100) | Internal |
|  | Overseas players to keep an eye for in baseball | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Player profiles for football | Football department’s servers | Football department | High($100-$1,000) | Confidential |
|  | Player profiles for basketball | Basketball department’s servers | Basketball department | High($100-$1,000) | Confidential |
|  | Player profiles for baseball | Baseball department’s servers | Baseball department | High($100-$1,000) | Confidential |
|  | Profiles on football organization | Football department’s servers | Football department | High($100-$1,000) | Confidential |
|  | Profiles on basketball organization | Basketball department’s servers | Basketball department | High($100-$1,000) | Confidential |
|  | Profiles on baseball organization | Baseball department’s servers | Baseball department | High($100-$1,000) | Confidential |
|  | Ranking of which teams will get what pick in the draft for football | Football department’s servers | Football department | High($100-$1,000) | Confidential |
|  | Ranking of which teams will get what pick in the draft for basketball | Basketball department’s servers | Basketball department | High($100-$1,000) | Confidential |
|  | Ranking of which teams will get what pick in the draft for baseball | Baseball department’s servers | Baseball department | High($100-$1,000) | Confidential |
|  | Number of venues owned by the company | Venue department’s servers | Venue department | Low($0-$10) | Public |
|  | Potential draft swaps for football | Football department’s servers | Football department | High($100-$1,000) | Confidential |
|  | Potential draft swaps for basketball | Basketball department’s servers | Basketball department | High($100-$1,000) | Confidential |
|  | Money spent in maintaining a selected venue | Venue department’s servers | Venue department | Medium($10-$100) | Internal |
|  | Revenue earned from a selected venue | Venue department’s servers | Venue department | Medium($10-$100) | Internal |
|  | Profit earned from a selected venue | Venue department’s servers | Venue department | Medium($10-$100) | Internal |
|  | Potential draft swaps for baseball | Baseball department’s servers | Baseball department | Medium($10-$100) | Internal |
|  | Total profit earned this year | Location servers in general headquarters | IT department of general headquarter | Medium($10-$100) | Internal |
|  | Total profit earned last year | Location servers in general headquarters | IT department of general headquarter | Medium($10-$100) | Internal |
|  | Stock worth this year | Location servers in general headquarters | IT department of general headquarter | Medium($10-$100) | Internal |
|  | Stock worth last year | Location servers in general headquarters | IT department of general headquarter | Medium($10-$100) | Internal |
|  | Profits earned in each quartile | Location servers in general headquarters | IT department of general headquarter | Medium($10-$100) | Internal |
|  |  |  |  |  |  |