Longhorn Ride

Information Security and Privacy

Name: Aditya Khanna
Last Amended: 9 May 2020

1 Change History

Date	Description of Change	Change Made By:
10 February 2020	Created the document purpose, audience description including stakeholders, and data inventory (description, elements, owners, and locations) with 204 entries	Aditya Khanna
21 February 2020	Updated purpose, updated audience description, updated data inventory description, created data classification scheme, created data valuation methodology, and summarized data asset statistics	Aditya Khanna
9 March 2020	Updated the purpose to include vulnerabilities and risks, described the importance of identifying vulnerabilities and risks in a general context, described the importance of identifying vulnerabilities and risks in the context of Longhorn Ride, created a classification diagram of vulnerabilities, created a matrix of vulnerabilities and associated risks, and calculated the estimated risk impact for the top two risks	Aditya Khanna
10 April 2020	Updated the purpose to include trusted identity and access controls, specified the access control design for Longhorn Ride, described the rationale behind the access control design, enumerated the types of stakeholders that require access, specified levels of assurance for stakeholder authentication, and created the access control specifications for each stakeholder type	Aditya Khanna
20 April 2020	Updated the purpose to include the incident response plan, explained the importance of defining security occurrences (security events, security incidents, and data breaches), explained the difference between security occurrences (security events, security incidents, and data breaches), constructed a table of possible security events, constructed a table of possible security incidents, constructed a table of possible data breaches, created a table that defines incident priority levels and their associated criteria, defined the incident response team (roles and	Aditya Khanna

	responsibilities), constructed an incident response notification plan	
9 May 2020	Updated the purpose to include information regarding the trust framework structure of Longhorn Ride as well as technology solutions that ensure information security, delineated the trust framework structure as well as its associated benefits and complexities, constructed a table of technology solutions for the selected trust framework, and constructed a solution set for network and web security	Aditya Khanna

2 Purpose

Longhorn Ride aspires to provide an efficacious transportation solution for the Austin area through our ride-sharing platform. Whether you are a student, an everyday professional, or a local resident, Longhorn Ride aims to get you where you need to be in a convenient and timely manner.

The purpose of this information security and privacy plan is to provide a comprehensive definition of our stakeholders, the information we collect, and the security protocols surrounding these data elements. We first enumerate the stakeholders of our intended audience; in order to appropriately track the movement and modification of significant data elements, it is imperative that we identify individuals from whom the data was gathered, individuals interested in the data, individuals that can access/modify the data, and individuals impacted by a potential information breach. These stakeholders (specifically the riders, drivers, internal employees, investors, and third-party vendors) shall be defined in the next section. By identifying these important demographics and establishing information privacy standards, we are able to ameliorate the security of Longhorn Ride and protect our stakeholders.

An important section of this information security and privacy plan is the data inventory that we define later in the document. Within the data inventory, we enumerate data elements, their locations within our organization, and their owners. This organized log of key information values allows us to track important data at all times. Not all information is weighted the same; information differs by importance and credibility. Additionally, data can be categorized by its risk concerns, its access concerns, and its protections. By categorizing the data elements according to these concerns within the data inventory, we are able to assess potential risks and vulnerabilities within our systems. This also allows us to avoid potential threats by appropriately investing in our system's security infrastructure. This ultimately reduces liability and ensures that stakeholder information is private and secure. Finally, the data inventory allows us to document changes and track data. This also improves security audit logs, which can increase the speed at which we respond to a breach of information. If a breach were to occur, we would be able to notify the impacted stakeholders and respond to the threat appropriately. Furthermore, the data inventory augments support for general business process designs and improves operational efficiencies.

We also categorize the data elements in the data inventory according to a classification scheme as well as a valuation methodology. The classification scheme has four categories: public, proprietary, confidential, and regulatory. The valuation methodology assigns a value to each of the data elements. These categorizations allow us to analyze the impact of a data breach as well as determine which individuals are impacted and how much financial value is potentially compromised. This allows us to group certain elements and invest in the security infrastructure of our data inventory appropriately – which minimizes risks and potential threats.

We also delineate vulnerabilities and potential risks associated with the information within our data inventory. Vulnerabilities are weaknesses within Longhorn Ride that can expose information; they can manifest within the processes, people, and systems of Longhorn Ride. Threats to our system can exploit such vulnerabilities and target our information. In an information security and privacy context, risks are potential losses and damages that occur when threats take advantage of system vulnerabilities. To begin, we describe the importance of identifying vulnerabilities and their associated risks in a general context. Next, we analyze the vulnerabilities and potential risks of Longhorn Ride. We then create a classification diagram of vulnerabilities, which describes general types of vulnerabilities. Finally, we create a matrix of vulnerabilities and associated risks. By identifying vulnerabilities, we are able to secure our systems by investing in system infrastructure more approximately, ameliorate business processes, educate individuals about cybersecurity, protect high-risk data as well as targeted assets, and mitigate risks. We can also identify what the primary threats to Longhorn are as well as how they can exploit the vulnerabilities of our system. Additionally, we can also estimate the risk impacts that would occur if our system is compromised and there is a breach of information.

In the next section, we describe the information security and privacy protocols that govern information access and sharing controls for Longhorn Ride. To begin, we implement an Attribute-Based Access Control (ABAC) design. We then explain the rationale behind our access control design and describe why it is the most appropriate structure for the Longhorn Ride infrastructure. Next, we enumerate the different types of stakeholders that interact with our systems and require access to different data components. Afterwards, we construct a table that delineates the levels of assurance for each stakeholder that determines authentication policies. This table includes the Identity Assurance Level (IAL), Token Assurance Level (TAL), and the Level of Assurance (LOA) as well as their associated justifications for each stakeholder. Finally, we construct the stakeholder access controls table, which specifies the control specifications required to manipulate information within the data inventory. This is important, for it allows us assign each stakeholder an appropriate level of clearance in order to access information within our system. Additionally, this allows us to secure private information, ensure that only the intended parties are able to modify sensitive data, mitigate the risk of data breach, and protect data elements in each phase of the identity life cycle.

In the following section, we construct an incident response plan for Longhorn Ride. To begin, we define security events, security incidents, and data breaches; we also explain the difference between each of them. Afterwards, we construct tables of possible security events, security incidents, and data breaches so that we are prepared to appropriately respond if any of them occur. In addition, we delineate possible losses and impacts to business continuity for each of these security occurrences. Next, we construct a table of incident priority levels and associated criteria; this allows us to differentiate between incidents and respond to higher priority occurrences appropriately. Afterwards, we define our incident response team. We define their roles and associated responsibilities. This allows us to recognize who must be contacted is a security event, security incident, or data breach occurs; it also allows us to divide responsibilities and responses so that the Longhorn Ride responds efficiently if there is such a security occurrence. Finally, we construct an incident response notification plan. We define who must be notified, how the notification occurs, and the upper bound for notification time for each of the incident priority levels. This allows us to respond efficiently and appropriately to different levels of security incidents. It also ensures that only the appropriate individuals are notified and told how to respond – which reduces confusion in the case of a security incident. By solidifying our incident response plan, we are able to respond swiftly, efficiently, and appropriately to security threats and incidents. This allows us to bolster the security of our system as well as protect all stakeholders.

Finally, we describe the technological solutions and structure that ensures the highest level of information security and privacy for Longhorn Ride. To begin, we delineate the most optimal trust framework structure as well as its associated benefits and complexities. Next, we describe the technology solutions and for data ate rest, data in transit, and access to data within our trust framework. Finally, we construct a solution set for network and web security. These solutions are specific design principles and technologies that protect the confidentiality, integrity, and availability of information. Additionally, it ensures information security and privacy for all stakeholders and data owners.

3 Audience

The intended audience for this information security and privacy plan includes all stakeholders associated with the data elements enumerated within the data inventory. The stakeholders are composed of individuals interested in our information, individuals from whom we gathered the data elements, individuals that are able to access such data, and individuals that would be impacted if there was an information breach.

Data elements belonging to different data owners and parties are also categorized into groups according to a classification scheme as well as a valuation methodology. This allows us to assess the risk and access concerns associated with the data; additionally, we are able to appropriately invest in the infrastructure of our systems in order to secure these elements. Finally, by evaluating the classification and valuation of the data, we are able to determine which data owners are impacted and what the potential financial losses are (for both the stakeholders as well as Longhorn Ride).

Definitions for the different stakeholder categories are listed below.

Data Owners:

Data owners are defined as individuals who are accountable for data elements; they are able to access and modify the data elements enumerated within the data inventory for Longhorn Ride. There are many individuals and groups that are classified as data owners:

- Customers/Riders
- Drivers
- Investors
- Internal Employees (Specifically the IT and HR Departments)
- Executive Company Board of Longhorn Ride

Third-Party Vendors:

In this context, third-party vendors are defined as businesses that help Longhorn Ride operate. They are business organizations that contribute to and are impacted by the services and data of Longhorn Ride. These third-party vendors include cloud storage vendors that house certain data elements.

External Entities:

External entities are defined as entities that are interested in the data elements or information security policies at Longhorn Ride. These include insurance companies as well as information security and privacy companies.

4 Data Inventory

The purpose of the data inventory is to track and organize key data elements that the business is built upon. A data inventory is important, for it increases the security and privacy of Longhorn Ride. By enumerating data elements, their location, and their primary owners, we are able to analyze potential risks and assess vulnerabilities within our security system. This allows us to increase the security and privacy of stakeholder information by avoiding potential threats. We are also able to document changes to the infrastructure of our security system, which improves the ability to maintain security audit logs. This allows us to reduce liability as well as appropriately respond to breaches of private information (by tracing back threats to the source and notifying the impacted stakeholders). In the data inventory for Longhorn Ride, we create separate data owner categories for drivers and employees; drivers are the individuals that allow the business to run by driving customers, while employees are the individuals that work internally within the company (such as those in the IT and HR departments). There are also multiple co-owners to most of the data elements because of information and privacy laws such as GDPR.

We also categorize the data elements according to a classification scheme and a valuation methodology. The classification scheme can be divided into four categories – public, proprietary, confidential, and regulatory. The classification scheme allows us to evaluate the risk and access concerns associated with the data. The valuation methodology determines the associated financial value of the data. These two categorizations allow us to group the data elements, avoid potential threats, appropriately invest in the security infrastructure of the system, and swiftly respond to data breaches.

Table 1. **Data Inventory**

#	Data Element	Location	Owner	Valuation	Classification
1	Customer/Rider Name	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$15.90	Public
2	Customer/Rider Phone Number	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$15.90	Public
3	Customer/Rider Email Address	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$15.90	Public
4	Customer/Rider Address	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
5	Customer/Rider Age	On-Premise (Digital)	IT Department and Riders	$96.10	Confidential

		Internal ITS Data Server			
6	Customer/Rider Date of Birth	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
7	Customer/Rider Credit Card Information	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$4,050.00	Regulatory
8	Customer/Rider Disability Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$15.90	Public
9	Customer/Rider Username	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
10	Customer/Rider Password	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
11	Customer/Rider Ride Rating	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$15.90	Public
12	Customer/Rider Ride History	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
13	Customer/Rider Current Location	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$4,050.00	Regulatory
14	Customer/Rider Gender	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$15.90	Public
15	Customer/Rider Bank Account Routing Information	On-Premise (Digital)	IT Department and Riders	$4,050.00	Regulatory

		Internal ITS Data Server			
16	Customer/Rider Emergency Contact Information	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$96.10	Confidential
17	Customer/Rider Account Security Questions	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
18	Customer/Rider Account Picture	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$15.90	Public
19	Customer/Rider Billing Address	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
20	Customer/Rider Rideshare Call History	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
21	Customer/Rider Promotional Codes	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$15.90	Public
22	Customer/Rider Number of Cancellations	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
23	Customer/Rider Pet Information	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
24	Customer/Rider Party Size	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
25	Customer/Rider Conversation	Off-Premise (Digital) Cloud Vendor	IT Department and Riders	$62.00	Proprietary

	Preference (Personal Settings)	ITS Data Server			
26	Customer/Rider Pick-Up Location	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
27	Customer/Rider Smoking Preference (Personal Settings)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
28	Customer/Rider Carpool Preference (Personal Settings)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
29	Customer/Rider Zip Code	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
30	Customer/Rider Destination	On-Premise (Digital) Internal ITS Data Server	IT Department and Riders	$96.10	Confidential
31	Customer/Rider Height	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$96.10	Confidential
32	Customer/Rider Weight	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$96.10	Confidential
33	Customer/Rider Ethnicity	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$96.10	Confidential
34	Customer/Rider Language Preference (Personal Settings)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
35	Customer/Rider Allergies	Off-Premise (Digital) Cloud Vendor	IT Department and Riders	$96.10	Confidential

		ITS Data Server			
36	Customer/Rider Rideshare Messages	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Riders	$62.00	Proprietary
37	Driver Name	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
38	Driver Phone Number	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
39	Driver Email Address	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
40	Driver Address	On-Premise (Physical) ITS Filing Cabinet	IT Department and Drivers	$96.10	Confidential
41	Driver Age	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$96.10	Confidential
42	Driver Date of Birth	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential
43	Driver Credit Card Information	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$4,050.00	Regulatory
44	Driver Disability Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
45	Driver Username	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential

46	Driver Password	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential
47	Driver Ride Rating	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
48	Driver Ride History	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
49	Driver Current Location	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential
50	Driver Gender	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
51	Driver Bank Account Routing Information	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$4,050.00	Regulatory
52	Driver Emergency Contact Information	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$96.10	Confidential
53	Driver Account Security Questions	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential
54	Driver Account Picture	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$15.90	Public
55	Driver Billing Address	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential

56	Driver Criminal History	On-Premise (Digital) Internal ITS Data Server	HR Department and Drivers	$96.10	Confidential
57	Driver Rideshare Call History	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
58	Driver Active Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
59	Driver Medical History	On-Premise (Physical) ITS Filing Cabinet	HR Department and Drivers	$96.10	Confidential
60	Driver Social Security Number	On-Premise (Physical) ITS Filing Cabinet	HR Department and Drivers	$4,050.00	Regulatory
61	Driver Employment History	On-Premise (Digital) Internal ITS Data Server	HR Department and Drivers	$96.10	Confidential
62	Driver Veteran Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Drivers	$96.10	Confidential
63	Driver Citizenship Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Drivers	$96.10	Confidential
64	Driver Work Authorization Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Drivers	$4,050.00	Regulatory
65	Driver Driver’s License Number	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential
66	Driver Number of Cancellations	Off-Premise (Digital) Cloud Vendor	IT Department and Drivers	$62.00	Proprietary

		ITS Data Server			
67	Driver Work Time Sheet	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Drivers	$62.00	Proprietary
68	Driver Employment Eligibility Verification (I-9)	On-Premise (Physical) ITS Filing Cabinet	HR Department and Drivers	$4,050.00	Regulatory
69	Driver Employee Identification Number (EIN)	On-Premise (Physical) ITS Filing Cabinet	HR Department and Drivers	$4,050.00	Regulatory
70	Driver Tax Form W-2	On-Premise (Physical) ITS Filing Cabinet	HR Department and Drivers	$4,050.00	Regulatory
71	Driver Tax Form W-4	On-Premise (Physical) ITS Filing Cabinet	HR Department and Drivers	$4,050.00	Regulatory
72	Driver Conversation Preference (Personal Settings)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
73	Driver Accident History	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential
74	Driver Rideshare Insurance	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$4,050.00	Regulatory
75	Driver Driving Distance Preference (Personal Settings)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
76	Driver Smoking Preference (Personal Settings)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
77	Driver Zip Code	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$96.10	Confidential

78	Driver Height	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$96.10	Confidential
79	Driver Weight	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$96.10	Confidential
80	Driver Ethnicity	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$96.10	Confidential
81	Driver Language Preference (Personal Settings)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
82	Driver Number of Proficient Languages	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
83	Driver Allergies	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$96.10	Confidential
84	Driver Rideshare Messages	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
85	Driver Employment Start Date	On-Premise (Digital) Internal ITS Data Server	HR Department and Drivers	$62.00	Proprietary
86	Driver Vehicle Insurance	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$62.00	Proprietary
87	Driver Vehicle License Plate Number	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$15.90	Public

88	Driver Vehicle Disability Accommodation	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
89	Driver Vehicle Maximum Capacity (Seat Count)	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
90	Driver Vehicle Color	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
91	Driver Vehicle Model	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
92	Driver Vehicle Toll Tag Number	On-Premise (Digital) Internal ITS Data Server	IT Department and Drivers	$4,050.00	Regulatory
93	Driver Vehicle Pet Accommodation	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$15.90	Public
94	Driver Vehicle Luggage Capacity	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
95	Driver Vehicle Bluetooth Compatibility	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
96	Driver Vehicle Self-Driving Capability	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
97	Driver Vehicle Electric/Hybrid Automobile Classification	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary

98	Driver Vehicle Height Clearance	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
99	Driver Vehicle Texas Registration Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
100	Driver Vehicle Inspection Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Drivers	$62.00	Proprietary
101	Employee Name	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$15.90	Public
102	Employee Phone Number	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$15.90	Public
103	Employee Email Address	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$15.90	Public
104	Employee Address	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
105	Employee Age	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$96.10	Confidential
106	Employee Date of Birth	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
107	Employee Credit Card Information	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$4,050.00	Regulatory

108	Employee Disability Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$96.10	Confidential
109	Employee Username	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
110	Employee Password	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
111	Employee Citizenship Status	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Employee	$96.10	Confidential
112	Employee Work Authorization Status	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$4,050.00	Regulatory
113	Employee Driver's License Number	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
114	Employee Gender	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Employee	$96.10	Confidential
115	Employee Bank Account Routing Information	On-Premise (Physical) ITS Filing Cabinet	IT Department and Employee	$4,050.00	Regulatory
116	Employee Emergency Contact Information	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$96.10	Confidential
117	Employee Account Security Questions	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
118	Employee Account Picture	On-Premise (Digital)	IT Department and Employee	$96.10	Confidential

		Internal ITS Data Server			
119	Employee Billing Address	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
120	Employee Criminal History	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
121	Employee Life Insurance	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
122	Employee 401(k) Information	On-Premise (Physical) ITS Filing Cabinet	HR Department and Employee	$4,050.00	Regulatory
123	Employee Medical History	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
124	Employee Social Security Number	On-Premise (Physical) ITS Filing Cabinet	HR Department and Employee	$4,050.00	Regulatory
125	Employee Employment History	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
126	Employee Veteran Status	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
127	Employee Salary	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
128	Employee Tax Form W-2	On-Premise (Physical) ITS Filing Cabinet	HR Department and Employee	$4,050.00	Regulatory
129	Employee Tax Form W-4	On-Premise (Physical)	HR Department and Employee	$4,050.00	Regulatory

		ITS Filing Cabinet			
130	Employee Work Time Sheet	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Employee	$96.10	Confidential
131	Employee Employment Eligibility Verification (I-9)	On-Premise (Physical) ITS Filing Cabinet	HR Department and Employee	$4,050.00	Regulatory
132	Employee's Employee Identification Number (EIN)	On-Premise (Physical) ITS Filing Cabinet	HR Department and Employee	$4,050.00	Regulatory
133	Employee Job Title	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Employee	$15.90	Public
134	Employee Education History	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Employee	$96.10	Confidential
135	Employee Zip Code	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
136	Employee Medical Insurance	On-Premise (Digital) Internal ITS Data Server	IT Department and Employee	$96.10	Confidential
137	Employee Height	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$96.10	Confidential
138	Employee Weight	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$96.10	Confidential
139	Employee Ethnicity	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$96.10	Confidential

140	Employee Number of Proficient Languages	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$62.00	Proprietary
141	Employee Allergies	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
142	Employee Employment Start Date	Off-Premise (Digital) Cloud Vendor ITS Data Server	IT Department and Employee	$62.00	Proprietary
143	Employee Blood Type	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
144	Employee Workspace Access Information	On-Premise (Physical) ITS Filing Cabinet	IT Department and Employee	$4,050.00	Regulatory
145	Employee Security Clearance (Internal for Company Use)	On-Premise (Physical) ITS Filing Cabinet	IT Department and Employee	$4,050.00	Regulatory
146	Employee Resume/CV	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
147	Employee Paid Time Off Amount	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$62.00	Proprietary
148	Employee Government Clearance (Government Related Projects)	On-Premise (Physical) ITS Filing Cabinet	IT Department and Employee	$4,050.00	Regulatory
149	Employee Number of Dependents (Spouses and Children)	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$96.10	Confidential
150	Employee Household Income	On-Premise (Digital)	HR Department and Employee	$96.10	Confidential

		Internal ITS Data Server			
151	Employee Visa Type	On-Premise (Digital) Internal ITS Data Server	HR Department and Employee	$4,050.00	Regulatory
152	Employee Location of Permanent Residence	Off-Premise (Digital) Cloud Vendor ITS Data Server	HR Department and Employee	$96.10	Confidential
153	Investor Name	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$62.00	Proprietary
154	Investor Phone Number	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$62.00	Proprietary
155	Investor Email Address	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$62.00	Proprietary
156	Investor Address	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$96.10	Confidential
157	Investor Bank Account Routing Information	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$4,050.00	Regulatory
158	Investor Total Equity/Stock Value	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$4,050.00	Regulatory
159	Investor Occupation	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$96.10	Confidential
160	Investor Relation to Longhorn Ride Company	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$62.00	Proprietary
161	Investor Investment Date	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$62.00	Proprietary
162	Investor Return on Investment Value	On-Premise (Physical) ITS Filing Cabinet	IT Department and Investor	$96.10	Confidential

163	Total Investment Contributions	On-Premise (Physical) ITS Filing Cabinet	IT Department	$96.10	Confidential
164	Paid Investments (Assets)	On-Premise (Physical) ITS Filing Cabinet	IT Department	$4,050.00	Regulatory
165	Unpaid Investments (Liabilities)	On-Premise (Physical) ITS Filing Cabinet	IT Department	$4,050.00	Regulatory
166	Potential Investor Names	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
167	Potential Investor Relation to Longhorn Ride Company	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
168	Potential Investor Phone Number	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
169	Potential Investor Email Address	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
170	Potential Investor Address	On-Premise (Physical) ITS Filing Cabinet	IT Department	$96.10	Confidential
171	Potential Investor Occupation	On-Premise (Physical) ITS Filing Cabinet	IT Department	$96.10	Confidential
172	Longhorn Ride Company Number of Registered Customers/Riders	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
173	Longhorn Ride Company Number of Registered Drivers	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
174	Longhorn Ride Company Number of Employees	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary

175	Longhorn Ride Company Number of Investors	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
176	Longhorn Ride Company Official Address (Headquarters)	On-Premise (Digital) Internal ITS Data Server	IT Department	$15.90	Public
177	Longhorn Ride Company Net Worth	On-Premise (Digital) Internal ITS Data Server	IT Department	$15.90	Public
178	Longhorn Ride Company Tax Identification Number	On-Premise (Physical) ITS Filing Cabinet	IT Department	$4,050.00	Regulatory
179	Longhorn Ride Company Liability Insurance	On-Premise (Physical) ITS Filing Cabinet	IT Department	$4,050.00	Regulatory
180	Longhorn Ride Company Internal Server Space/Memory Capacity (Digital)	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
181	Longhorn Ride Company Stock Value	On-Premise (Physical) ITS Filing Cabinet	IT Department	$4,050.00	Regulatory
182	Longhorn Ride Company Yearly Revenue	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
183	Longhorn Ride Company Number of Office Locations	On-Premise (Digital) Internal ITS Data Server	IT Department	$15.90	Public
184	Longhorn Ride Company Cyber Insurance Policy	On-Premise (Digital) Internal ITS Data Server	IT Department	$4,050.00	Regulatory
185	Longhorn Ride Company Number of Employee Computers	On-Premise (Digital) Internal ITS Data Server	IT Department	$96.10	Confidential

186	Longhorn Ride Company Employee Computer Identification Numbers	On-Premise (Physical) ITS Filing Cabinet	IT Department	$4,050.00	Regulatory
187	Longhorn Ride Company Internal Filing Space Capacity (Physical)	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
188	Longhorn Ride Company iOS Application Identification Number	On-Premise (Digital) Internal ITS Data Server	IT Department	$4,050.00	Regulatory
189	Longhorn Ride Company Android Application Identification Number	On-Premise (Digital) Internal ITS Data Server	IT Department	$4,050.00	Regulatory
190	Longhorn Ride Company Number of iOS Application Downloads	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
191	Longhorn Ride Company Number of Android Application Downloads	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
192	Longhorn Ride Company Annual Cost of Hosting Application on iOS Store	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
193	Longhorn Ride Company Annual Cost of Hosting Application on Android Store	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
194	Longhorn Ride Company Estimated Market Share Value for Rideshare Service	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
195	Longhorn Ride Company Website Domain Name	On-Premise (Digital) Internal ITS Data Server	IT Department	$15.90	Public

196	Longhorn Ride Company Website Traffic Value	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
197	Longhorn Ride Company Number of Transactions on Website	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
198	Longhorn Ride Company Number of Transactions on iOS Application	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
199	Longhorn Ride Company Number of Transactions on Android Application	On-Premise (Physical) ITS Filing Cabinet	IT Department	$62.00	Proprietary
200	Third-Party Cloud Storage Vendor Name	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
201	Third-Party Cloud Storage Vendor Storage/Memory Capacity	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
202	Third-Party Cloud Storage Vendor Contract Length	On-Premise (Digital) Internal ITS Data Server	HR Department	$62.00	Proprietary
203	Third-Party Cloud Storage Vendor Annual Cost	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary
204	Third-Party Cloud Storage Vendor Bandwidth	On-Premise (Digital) Internal ITS Data Server	IT Department	$62.00	Proprietary

5 Information Valuation and Categorization

Data Classification Scheme:

A data classification scheme is a fundamental way to organize information within our data inventory, for it allows us to analyze the risk, protection, and access concerns associated with the data elements. This organizational structure allows us to develop the foundation of our information security and privacy infrastructure. This classification also helps us determined what security protocols are required by each data element; additionally, it allows us to appropriately respond to the data owners in the circumstance that there is a breach. A data classification scheme indicates where valuable information within our data inventory resides; the valuation methodologies (which are defined in the next section) and the financial values of this information are based on this classification scheme.

Table 2. **Classification Scheme Categories**

Public Data	Public data is associated with the highest level of accessibility as well as the lowest level of risk. Unauthorized modification of the data would result in minimal harm to data owners and Longhorn Ride. Such information includes the location of the Longhorn Ride headquarters or general information such as brand names.
Proprietary Data	Proprietary data is private data that is associated with a low level of accessibility as well as a low level of risk. Unauthorized modification of the data would result in a reduced competitive advantage for Longhorn Ride. Such information includes private company information such as the number of users as well as the number of investors.
Confidential Data	Confidential data is private data that is associated with a low level of accessibility as well as a high level of risk. Unauthorized modification of this restricted information would result in damage to data owners and Longhorn Ride. Such information includes personal data such as rider and driver information.
Regulatory Data	Regulatory data is private data that is associated with the lowest level of accessibility as well as the highest level of risk; it requires the highest level of integrity. Unauthorized modification of this highly sensitive information would result in serious damage to data owners and Longhorn Ride. Such information includes Social Security Numbers, internal company tax information, and undisclosed projects.

The rationale for choosing this classification scheme is based on the potential impact on data owners and Longhorn Ride under the circumstance of a data breach. The classifications that we have selected (public, proprietary, confidential, and regulatory) allow us to categorize data elements in a simple yet efficacious manner. This allows us to determine the security infrastructure needed for each classification as well as the financial values of the information.

Data Valuation Methodology:

The valuation methodology that we use to calculate the data asset valuation for the elements in the data inventory is influenced by incurred loss, creation value, replacement value, monetization value, data age, data volume, data periodicity, and data accuracy variables. The value of the information is calculated from the perspective of our company, Longhorn Ride. The specific data asset valuation equation that we use for the valuation methodology of Longhorn Ride is derived from the data value equation defined within “A Pricing Model for Data Markets”, which is a market study conducted by the UC Berkeley School of Information (Heckman et al. 7).

Our specific data asset valuation for Longhorn Ride is delineated below; it is rationale, transparent, and repeatable for all of the elements within our data inventory.

$$\boxed{\begin{aligned} & \mathit{Data\ Asset\ Valuation} \\ &\qquad = \big((\mathit{Creation\ Value} * \mathit{Data\ Volume}) + \mathit{Replacement\ Value} \\ &\qquad + (\mathit{Monetization\ Value} * \mathit{Data\ Age} * \mathit{Data\ Periodicity})\big) * \mathit{Data\ Accuracy} \\ &\qquad + \mathit{Incurred\ Loss} \end{aligned}}$$

The valuations of the data elements are grouped by the classification scheme categories (public, proprietary, confidential, and regulatory) enumerated within the previous section. The rationale for choosing this valuation methodology is based on the potential impact on data owners and Longhorn Ride under the circumstance of a data breach. The value of the data is dependent on the potential liabilities (incurred loss) plus the raw value of the data (a calculation involving creation cost of the data, the volume of the data, the replacement cost of the data, the periodicity of the data, the age of the data, and the monetization of the data) times the accuracy of the data. If the data is not accurate to begin with, the value is decreased. If the potential liability is high, the value is increased.

The precision of the variables used for the data asset valuation calculation is separated by classification scheme groupings. The precision for these groups (public, proprietary, confidential, and regulatory) is embedded within their expected values listed below.

The variables used for the data asset valuation equation are listed below; by defining them, we are able to make the calculation rationale, transparent, and repeatable for all of the elements within our data inventory.

Incurred Loss:

The incurred loss value is the sum of loss incurred by the data holders, the loss incurred by Longhorn Ride, potential legal actions taken after a breach, and the financial cost of users that no longer use our rideshare platform. The estimated value of incurred loss for each classification category is listed below.

- Public Data: $0.50
- Proprietary Data: $1
- Confidential Data: $10
- Regulatory Data: $100

Creation Value:

The creation value is the cost to create, collect, and verify a particular data element. The estimated value of creation value for each classification category is listed below.

- Public Data: $1
- Proprietary Data: $1
- Confidential Data: $10
- Regulatory Data: $100

Replacement Value:

The replacement value is the cost to replace or recover a particular data element. The estimated replacement value for each classification category is listed below.

- Public Data: $1
- Proprietary Data: $10
- Confidential Data: $10
- Regulatory Data: $100

Monetization Value:

The monetization value is the financial value that a criminal entity can acquire from a particular data element. The estimated replacement value for each classification category is listed below.

- Public Data: $1
- Proprietary Data: $10
- Confidential Data: $10
- Regulatory Data: $1000

Data Periodicity:

The data periodicity is the number of days a particular data element is used within a year; it can range from 0-1. The estimated value of data periodicity for each classification category is listed below.

- Public Data: 1
- Proprietary Data: 1
- Confidential Data: 0.5
- Regulatory Data: 0.25

Data Volume:

The data volume is the number of instances of a particular data element. The estimated value of data volume for each classification category is listed below.

- Public Data: 1
- Proprietary Data: 1
- Confidential Data: 1.3 (Due to Expected Values of 1 or More Instances – Skewed Towards 1)
- Regulatory Data: 1

Data Age:

The data age is the number of years that a particular data element has existed since it was created. The estimated value of data age for each classification category is listed below.

- Public Data: 20
- Proprietary Data: 5
- Confidential Data: 20
- Regulatory Data: 15

Data Accuracy:

The data accuracy is a value from 0-1 that denotes the probability that a particular data element is accurate. The estimated value of data accuracy for each classification category is listed below.

- Public Data: 0.7
- Proprietary Data: 1
- Confidential Data: 0.7
- Regulatory Data: 1

Since the valuation methodologies are grouped by the classification scheme categories, we have listed the data asset valuation for each category below. These data asset valuations can be found in the data inventory table next to their respective data elements.

Valuation of Public Data:
Data Asset Valuation = ((1*1) + (1) + (1*20*1))*(0.7) + 0.50
Data Asset Valuation = $15.90

Valuation of Proprietary Data:
Data Asset Valuation = ((1*1) + (10) + (10*5*1))*(1) + 1
Data Asset Valuation = $62.00

Valuation of Confidential Data:
Data Asset Valuation = ((10*1.3) + (10) + (10*20*0.5))*(0.7) + 10
Data Asset Valuation = $96.10

Valuation of Regulatory Data:
Data Asset Valuation = ((100*1) + (100) + (1000*15*0.25))*(1) + 100
Data Asset Valuation = $4050.00

<u>Summary of Data Assets:</u>

Table 3. **Percentage of Data in Classification Categories and Their Associated Valuations**

	Public	Proprietary	Confidential	Regulatory	Total
Number of Elements	26	66	75	37	204
Percentage of Data	12.745%	32.353%	36.765%	18.137%	100%
Valuation Per Data Element	$15.90	$62.00	$96.10	$4,050.00	N/A
Valuation for Classification Category	$413.40	$4,092.00	$7,207.50	$149,850.00	$161,562.90

Table 4. **Valuation of Information for Data Owners**

	Number of Public Elements	Number of Proprietary Elements	Number of Confidential Elements	Number of Regulatory Elements	Valuation Per Individual Data Owner
Rider/Customers	**8**	**10**	**15**	**3**	**$14,338.70**
Drivers	**10**	**23**	**21**	**10**	**$44,103.10**
Internal Employees	**4**	**3**	**32**	**13**	**$55,974.8**
Investors	**0**	**9**	**6**	**2**	**$9,234.60**
Other	**4**	**21**	**1**	**9**	**37,911.70**

We estimate that we will have approximately 7,000 customers/riders, 500 drivers, 300 internal employees, and 100 investors. With this approximation of stakeholders and data owners, we can calculate the total valuation of information. By multiplying the valuations per individual data owner (calculated in Table 4) by the number of data owners and adding a single value of the other miscellaneous data elements, we are able to create a calculation to accurately model the total valuation of information for Longhorn Ride; this mathematical model is illustrated below.

$$
\begin{aligned}
&Total\ Valuation \\
&\quad = (Number\ of\ Riders * Valuation\ of\ Riders) \\
&\quad + (Number\ of\ Riders * Valuation\ of\ Riders) \\
&\quad + (Number\ of\ Riders * Valuation\ of\ Riders) \\
&\quad + (Number\ of\ Riders * Valuation\ of\ Riders) + (Other\ Valution)
\end{aligned}
$$

Thus, according to this equation, the total valuation of information for Longhorn Ride is $140,176,261.70 (with 7,000 customers/riders, 500 drivers, 300 internal employees, and 100 investors).

$$\boxed{\textit{Total Valuation of Information for Longhorn Ride} = \$140,176,261.70}$$

Groupings:

The data elements within the data inventory form groupings according to their respective valuations. These groupings parallel the classification scheme categories (public, proprietary, confidential, and regulatory). The categories can be grouped into public and private data. Private data includes proprietary, confidential, and regulatory data. Public data usually includes easily accessible information; the valuation of such information is the lowest. Proprietary data includes information with a low level of accessibility as well as a low level of risk; the valuation of such information is higher than that of public data. Confidential data includes information with a low level of accessibility as well as a high level of risk; the valuation of such information is higher than that of proprietary data. Finally, regulator data is the most sensitive type of information; the valuation of such information is the highest of the groups.

These groupings also support the idea that data elements have different values to different groups and populations. For instance, rider and driver data owners value their personal information more highly than Longhorn Ride company information. In contrast, investors care more about company statistics than rider information. This division in groupings and valuations can be seen across data owners.

Correlations:

There is a clear correlation between the classification scheme categories and their associated valuations. As the information becomes more sensitive, the valuation of the data elements increases; this means that data elements with a high level of risk and low level of accessibility are calculated to have the highest valuations. This correlation is seen in both Table 1 and Table 3.

The group of public data has a valuation of $15.90 per data element; it includes easily accessible information such as names and phone numbers. The group of proprietary data has a valuation of $62.00 per data element; it includes information such as company statistics and metrics. The group of confidential data has a valuation of $96.10 per data element; it includes personal information such as medical records. The group of regulatory data has a valuation of $4050.00 per data element; it includes government information such as social security numbers and tax data.

References:

Barton, T. “Data Classification Guide.” *Information Technology Services*, The University of Chicago, https://its.uchicago.edu/data-classification-guideline/. Accessed 19 February 2020.

Heckman, Judd, et al. “A Pricing Model for Data Markets.” *BAIR*, UC Berkeley School of Information, https://www.ideals.illinois.edu/bitstream/handle/2142/73449/207_ready.pdf?sequence=2. Accessed 19 February 2020.

Jia, Ruoxi. “What is My Data Worth?” *BAIR*, Berkeley Artificial Intelligence Research, https://bair.berkeley.edu/blog/2019/12/16/data-worth/. Accessed 19 February 2020.

Markiewicz, Doug, et al. “Guidelines for Data Classification.” *Information Security Office - Computing*, Carnegie Mellon University, www.cmu.edu/iso/governance/guidelines/data-classification.html. Accessed 19 February 2020.

Thomas, Eck. “7 Steps to Effective Data Classification.” *SIRIUS*, SIRIUS Edge, https://edge.siriuscom.com/security/7-steps-to-effective-data-classification. Accessed 19 February 2020.

6 Vulnerabilities and Risks

Importance of Identifying Vulnerabilities and Risks:

Identifying vulnerabilities and potential risks is an important step in ensuring information security and privacy. Vulnerabilities are defined as weaknesses that can manifest within the systems, processes, and people of an organization; when exploited, data could be breached, private information could be exposed, and assets could be damages. Risks are potential losses and damages that occur when threats exploit the vulnerabilities of an organization. By identifying vulnerabilities and risks at a company, we are able to minimize liabilities as well as identify potential threats and their respective sources. Additionally, we could bolster vulnerabilities at the point of their origin; we can appropriately invest in the infrastructure of our system, improve the security of our business procedures, and educate individuals about cybersecurity. Finally, we can construct an appropriate plan of action as well as calculate risk impacts for the instance in which our system is compromised and there is a breach of information.

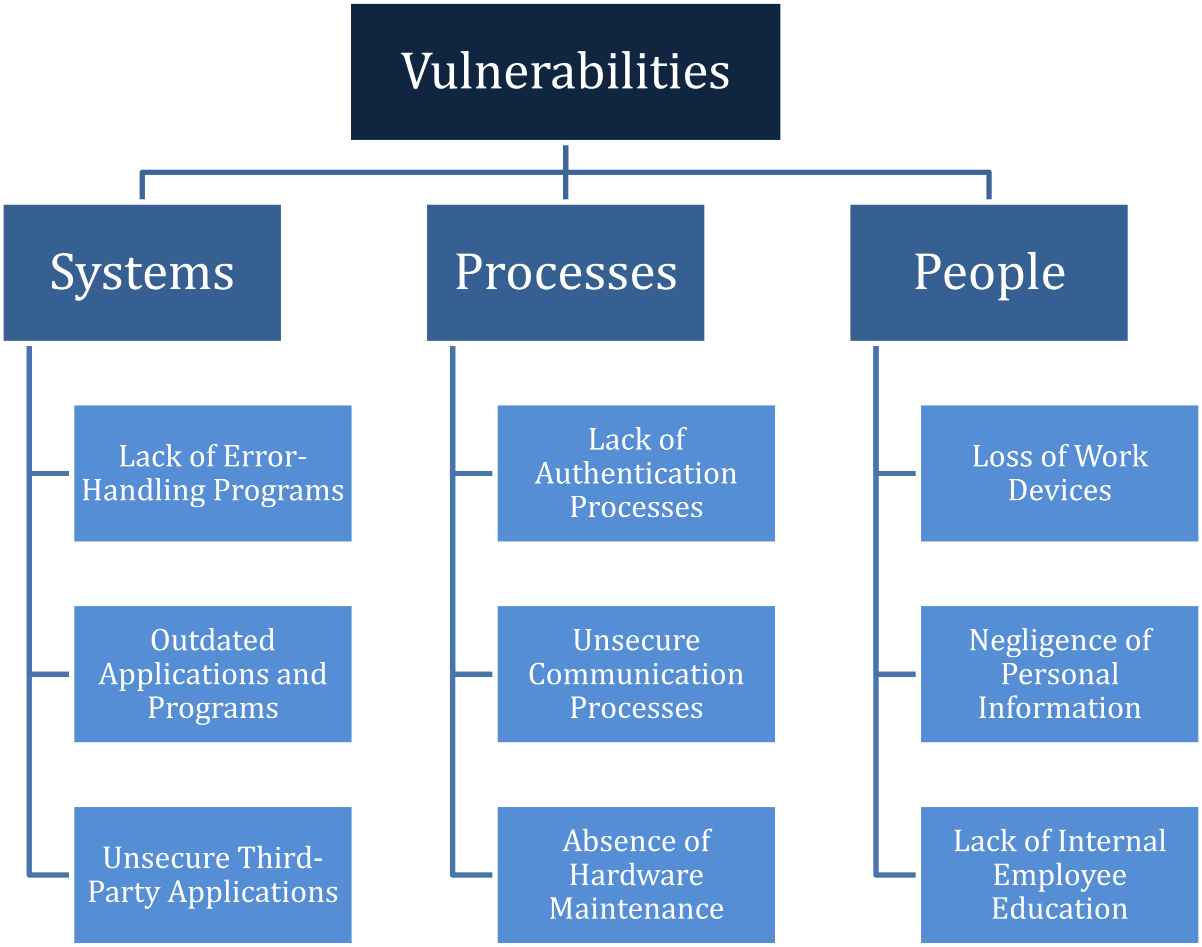
For Longhorn Ride specifically, it is important to identify vulnerabilities and risks in order to protect data owners (such as customers/riders, drivers, investors, internal employees, and company executives), third-party vendors, and external entities. By analyzing vulnerabilities and their associated risks, we are able to strengthen the security protocol surrounding important information as well as determine potential threats. This allows us to create an internal rideshare system that maintains confidentiality, integrity, and availability of our information. In accordance with our valuation methodology, our vulnerability matrix will allow us to pinpoint high-risk data and address vulnerabilities for such information. This could include securing the transfer of rider and driver information through our rideshare application in order to ensure personal information (such as names or credit card information) is not accessible by unauthorized parties. This could also include protecting internal company information (such as administrative login credentials or physical device data) in order to ensure that internal employee information as well as investor information is not leaked. We are also able to estimate liabilities associated with information within our data inventory. If Longhorn Ride data was breached, we could calculate the legal costs, labor costs, general emotional distress for involved parties, and damage to the company's reputation. This allows us to respond appropriately in the event that our system is compromised as well as forecast potential liabilities – which could influence the valuation and structure of our business.

The following classification diagram of vulnerabilities and matrix of vulnerabilities and associated risks will allow us to identify vulnerabilities as well as determine their risk levels. This organization scheme allows us to appropriately allocate resources in order to ensure information security and privacy.

<u>Classification Diagram of Vulnerabilities:</u>

Vulnerabilities are weaknesses that can be exploited by threats; they are manifested within the systems, processes, and people of Longhorn Ride. These vulnerabilities are further categorized into nine general vulnerabilities in our classification diagram below; they are the leaf nodes.

Figure 1. **Classification Diagram of Vulnerabilities**


Vulnerabilities
Systems
Processes
People
Lack of Error-Handling Programs
Outdated Applications and Programs
Unsecure Third-Party Applications
Lack of Authentication Processes
Unsecure Communication Processes
Absence of Hardware Maintenance
Loss of Work Devices
Negligence of Personal Information
Lack of Internal Employee Education

Matrix of Vulnerabilities and Associated Risks:

The matrix of vulnerabilities and associated risks is an important organization methodology that allows us to identify general vulnerabilities, their associated risks, and the overall impact on Longhorn Ride if such a vulnerability was exploited by threats. Vulnerabilities are weaknesses that can be located within the systems, processes, and people of Longhorn Ride; they are classified into nine general categories within our matrix. The systems vulnerabilities can be categorized into vulnerabilities due to a lack of error-handling programs, vulnerabilities due to outdated applications and programs, and vulnerabilities due to unsecure third-party applications. The processes vulnerabilities can be categorized into vulnerabilities due to a lack of authentication processes, vulnerabilities due to unsecure communication processes, and vulnerabilities due to an absence of hardware maintenance. The people vulnerabilities can be categorized into vulnerabilities due to a loss of work devices, vulnerabilities due to negligence of personal information, and vulnerabilities due to a lack of internal employee education on cybersecurity policies. The matrix of vulnerabilities and associated risks allows us to analyze the highest level of risks and their potential impacts on Longhorn Ride. Additionally, we are able to identify the most significant vulnerabilities. This also allows us to trace threats to source by monitoring the vulnerabilities that are most targeted. With such insight, we are able to appropriately invest in our infrastructure in order to mitigate risks and deter threats. The consequences of a data breach include financial losses, damages to company reputation, emotional distress, incurred costs of labor, and overall company devaluation. A breach of information would impact all data owners (customers/riders, drivers, investors, internal employees, and company executives). For example, a breach in administrative credentials by a criminal organization could result in financial fraud for riders as well as drivers, financial loss for investors, impersonations of internal employees, and revoked access privileges for company executives. The vulnerabilities matrix allows us to effectively identify and address vulnerabilities as well as minimize potential liabilities for all parties.

Table 5. **Matrix of Vulnerabilities and Associated Risks**

	Type of Vulnerability	**Description of Specific Vulnerability Occurrence (Attack on the Vulnerability)**	**Risk Posed by Vulnerability (Impact Caused by Threat When Vulnerability Exploited)**	**Risk Level (High, Medium, Low)**
1	Lack of Error-Handling Programs	1.1) An individual exceeds the capacity of the buffer and begins to modify nearby locations in memory. This is known as a buffer overflow. This can occur when a user unintentionally exceeds the capacity of a certain text field and modifies other memory locations. This can	Confidentiality: The individual (user or hacker) is able to access nearby memory locations. This allows the individual to access and copy information without the appropriate authorization; they can bypass implemented	Risk Level: High risk level for Confidentiality, Integrity, and Availability. Justification: If the data within the adjacent memory locations is

		also occur when a criminal uses a program to overflow the system’s buffer size and access/modify adjacent information.	authentication protocols. Integrity: The individual (user or hacker) is able to modify the adjacent spaces in memory without the appropriate authorization. They can bypass implemented authentication protocols and overwrite information. Availability: The individual (user or hacker) interrupts the system’s intended access time by overflowing the buffer. They are not in the correct format when modifying the system and overwriting the adjacent memory locations. The vulnerability of an overflow buffer impacts the availability of the data. This also means certain information is now permanently unavailable.	important, access and modification caused by a buffer overflow poses a high level of risk. Suppose that a hacker has the knowledge of where administrative credentials are located in memory. Then they can overflow the buffer in that area and overwrite the administrative credentials. This then allows the hacker to modify the system at an administrative level (with the appropriate authorization and through the required authentication procedures). A hacker may then exploit these data elements for criminal activities.
		1.2) An individual executes shell commands on a restricted server. This is known as an OS command injection. An individual can then modify file privileges, access information on the	Confidentiality: The individual (user or hacker) is able to run shell commands on the operating system of the server that allows them	Risk Level: High risk level for Confidentiality, Integrity, and Availability.

		server, and modify the system itself.	to access previously restricted information. Integrity: Running shell commands on a server allows individuals to change the file privileges. This means information can now be modified and transmitted. Availability: An OS injection interrupts the normal flow of the system; it does not access system information at the intended time or format. This violates the availability of the information affected by the OS injection. Information can also be made unavailable to other network administrators.	Justification: An OS injection allows individuals to access all information on the server. This includes high-profile information such as payment information, SSN's, and personal information. Criminals are able to exploit this vulnerability to bypass the authentication protocols and obtain fraudulent authorization statuses. This allows them to steal and abuse such information for their gain.
		1.3) A hacker intercepts and influences a query request that the system executes on its associated database. This is known as an SQL injection. A hacker is then able to retrieve, access, and modify restricted information – which bypasses the required authentication protocols.	Confidentiality: The hacker is able to access information through the database and bypass the necessary authentication protocols within the system itself. Integrity: The hacker is able to bypass system requirements (for authorization and authentication) and modify information	Risk Level: High level of risk for Confidentiality and Integrity. Medium level of risk for Availability. Justification: SQL injections allow hackers to bypass the authentication procedures of the system completely

			directly through the database. This compromises integrity. Availability: The hacker interferes with the information before it reaches the system in an inappropriate format (a database format). This violates information.	and access the data through the database (without the necessary authorization). They can access any stored information such as PII and company information that can damage the overall valuation of Longhorn Ride (and harm all data owners).
2	Outdated Applications and Programs	2.1) The system utilizes an outdated firewall (an application that prevents unauthorized network access) on all of its networks. This allows hackers to bypass authentication protocols without the appropriate level of authorization.	Confidentiality: Hackers are able to bypass the outdated firewall and access private information. Integrity: After bypassing the firewall, hackers are able to grant themselves authorization privileges, which allow them to modify and transmit information. Availability: Hackers are able to render information unavailable by modifying the authorizations of other individuals. This interrupts the access time and format of the information for the whole system.	Risk Level: High level of risk for Confidentiality, Integrity, and Availability. Justification: An outdated firewall can result in a system-wide breach of information. Once hackers are able to bypass the outdated firewall, they can access and modify information without any authorization (and they need not verify their identities). This can lead to system exploitations and

				information theft (of all data on the current network).
		2.2) The system is constructed with outdated programs and algorithms. Individuals can abuse the structural vulnerabilities of the digital system to access as well as modify information. For instance, a hacker may abuse procedural code that does not express data encapsulation; they would be able to manipulate the data and influence other programs within the system.	Confidentiality: Individuals are able to take advantages of structural vulnerabilities within the system to access information and copy values. Integrity: Individuals can influence internal pieces of code by taking advantage of structural vulnerabilities. This allows them to indirectly modify and alter data elements throughout the system – to a limited degree. Availability: Hackers are able to modify certain data elements and render certain programs and pieces of code unavailable. Although it may not impact the entire system, certain information is made unavailable.	Risk Level: Medium level of risk for Confidentiality, Integrity, and Availability. Justification: Taking advantage of structural vulnerabilities allows hackers to access and modify certain information. They, however, do not have access to all of the information across the entire system. This means that the range of damage that can be done with the compromised system is limited.
3	Unsecure Third-Party Applications	3.1) The third-party cloud-storage vendor used by Longhorn Ride has no security protocols and is breached. Individuals are able to access system information and data elements through the third-party application and	Confidentiality: Individuals are able to access restricted information through the third-party application, which provides a back-door into the Longhorn Ride system.	Risk Level: High level of risk for Confidentiality, Integrity, and Availability. Justification: Individuals can manipulate

		completely bypass Longhorn Ride systems.	Integrity: Individuals are able to modify and transmit information directly within the cloud-storage database without going through the required authentication process of Longhorn Ride systems. Availability: Individuals can alter data elements and interfere with the database connection to Longhorn Ride servers. This can result in all information being unavailable, which causes the Longhorn Ride application to effectively shut down.	information directly through the third-party cloud storage vendor without the appropriate authorization and bypass the authentication protocols. They can directly access all information and exploit all data owners. This is a system-wide breach of information.
		3.2) Hackers intercept API calls for geolocation services. Hackers are able to access current personal information for riders/customers through the third-party application and are able to bypass Longhorn Ride authentication protocols.	Confidentiality: Hackers are able to access current personal information such as location and destination by exploiting weaknesses in the third-party system. Integrity: Hackers can intercept API calls and alter the transmission of information. By attacking the third-party application, hackers can request information and modify such information in the responses.	Risk Level: Medium level of risk for Confidentiality, Integrity, and Availability. Justification: Hackers can interfere with API calls between the Longhorn Rode system and third-party applications. They can steal current information from riders such as current location

			Availability: Altering API calls can render information unavailable for riders, drivers, and internal employees. Criminals can exploit such information while it is unavailable, especially due to the large lag time.	and other transmitted information. Although they cannot access all information across Longhorn Ride, they are able to abuse such information for personal gain.
4	Lack of Authentication Processes	4.1) There is no username and password required for administrative processes. There is no authentication procedure required to become an administrator. Hackers can exploit this vulnerability in order to access and modify information.	Confidentiality: Hackers can become authorized individuals with no identity proofing. This allows them to access all information across the system. Integrity: As administrators, hackers are able to modify and alter information. They can also set privileges for everybody on the system. Availability: Hackers are now able to revoke the accesses of other administrators and take control of the entire system. In this state, information will become unavailable as the hackers exploit the data.	Risk Level: High level of risk for Confidentiality, Integrity, and Availability. Justification: Hackers can become authorized individuals within the context of the system without identity proofing. This allows them to access and modify all information throughout the entire system. They are also able to revoke the privileges of other administrators, which can suspend the operations of the entire system. This is a high level of risk because all

				information across the system is compromised.
		4.2) There is no multi-factor authentication process to log into the Longhorn Ride application for drivers. A hacker is able to obtain the login credentials of a driver.	Confidentiality: Hackers can abuse the single authentication process required for drivers and access driver as well as rider information. Integrity: Hackers are also able to modify information for drivers that the fraudulently login as. This violates the integrity of driver information. Availability: Hackers are able to make certain driver information unavailable. They, however, cannot impact other drivers and riders (those of which have not been compromised).	Risk Level: Medium level of risk for Confidentiality and Integrity. Low level of risk for Availability. Justification: Hackers can only influence certain drivers. They are also unable to access and manipulate information of other drivers as well as riders. This means that the data breach is not system-wide.
		4.3) There is no authentication process for the database where Longhorn Ride information is stored. Individuals can directly access stored information within the database.	Confidentiality: Individuals may access information directly through the database and view restricted information. They are able to bypass the system authentication procedures by accessing the database directly. Integrity: Individuals are also able to modify and manipulate information directly through the	Risk Level: High level of risk for Confidentiality, Integrity, and Availability. Justification: An unsecured database allows hackers to bypass authentication protocols and access sensitive information without the

			database. That means previously restricted information can be modified and information integrity throughout the system is compromised. <u>Availability:</u> Individuals can also make information unavailable and permanently delete entries within the database. This means the Longhorn Ride application will not be able to access its data elements and will shut down.	proper authorization. They are able to view and alter information throughout the entire system, which explains why this vulnerability has a high level of risk.
5	Unsecure Communication Processes	5.1) Information is not encrypted when it is transmitted across Longhorn Ride networks. Hackers are able to intercept these packets of information and view them.	<u>Confidentiality:</u> Hackers are able to access information on the network by intercepting transmitted packets of data. They can view and access all information that is transmitted. <u>Integrity:</u> Hackers are also able to modify the information that is transmitted to the next location. They can intercept a packet of information at one stage and transmit an entirely different packet of information to the next stage.	<u>Risk Level:</u> High level of risk for Confidentiality, Integrity, and Availability. <u>Justification:</u> Hackers are able to intercept transmitted packets of data at certain network nodes. They are then able to view and modify the intercepted information before it is transmitted to the next location. This has a high risk because network

			Availability: Hackers are able to transmit fraudulent or spoof information that can make breached information unavailable. Hackers are then able to abuse that information while it is unavailable to the system.	attacks are usually undetected.
		5.2) Internal employees communicate sensitive information through non-work channels. These channels lack verification procedures and can be easily intercepted by hackers.	Confidentiality: Hackers are able to join these non-work channels without verifying their identity. They are then able to view the information that is transmitted across the unsecure channel.	Risk Level: Low level of risk for confidentiality. Justification: Hackers are able to infiltrate channels without encryption and access information that is communicated by internal employees. They, however, can only access information that has been discussed. Additionally, they cannot affect the integrity or availability of the information.
		5.3) Internal employees discuss private information in public. Individuals are able to hear sensitive information through a public medium.	Confidentiality: Individuals that eavesdrop on these conversations can identify PII and access information in a physical context.	Risk Level: Low level of risk for Confidentiality and Availability. Justification: Individuals are

			Availability: Malicious individuals can also harass or kidnap internal employees so that the information does not return to Longhorn ride facilities. Availability is only compromised when the information mentioned was never transmitted previously.	able to overhear conversation regarding private information. This compromises confidentiality primarily – given that the individuals that eavesdrop can influence the system. Availability is also affected when the information does not return to Longhorn Ride.
6	Absence of Hardware Maintenance	6.1) Internal employees do not adequately oversee the servers and the physical space where they reside. The servers overheat and start a fire. Information stored on the servers is lost and the Longhorn Ride shuts down.	Integrity: Data elements located on the servers is now destroyed. If it was not backed up earlier, that information is permanently lost – an irreparable modification. Availability: The information stored on the servers becomes unavailable until it is retrieved from cloud-storage. If it was not previously backed up, the information is now permanently unavailable. The application for Longhorn Ride also shuts down and becomes unavailable.	Risk Level: High level of risk for Integrity and Availability. Justification: Although this vulnerability is rarely intentional, it has a high level of risk, for information stored on local servers in a physical space can be lost. This directly impacts the business of Longhorn Ride as well as the data owners.
		6.2) The wires that connect physical electrical devices	Availability: If a server or important physical	Risk Level: Medium level of

		and servers are old and not maintained. Over time they become loose and unreliable. Once a wire is disconnected, the Longhorn Ride application shuts down and information is temporarily unavailable.	electrical device is disconnected, information on that device will become unavailable. This also means that the application itself will become unavailable.	risk for Availability. Justification: When a wire is disconnected, the Longhorn Ride application and its associated information becomes unavailable. This, however, is only temporary, for the systems will go live again after the wire is replaced. There is no loss of information and data is not accessed/modified during this time.
7	Loss of Work Devices	7.1) An internal employee loses an RFID (radio-frequency identification device). A hacker obtains this device and uses it to log into the system as an administrator.	Confidentiality: The hacker is able to obtain the login credentials of an administrator and access information throughout the system. Integrity: The hacker is impersonating an administrator on the network and is able to modify as well as transmit information throughout the system. Availability: The hacker can change file access privileges for other individuals as an	Risk Level: High level of risk for Confidentiality, Integrity, and Availability. Justification: The hacker is able to impersonate the internal employee (an administrator). This allows the hacker to access, modify, and change the availability of information throughout the system. They have

			administrator and make the information unavailable.	system-wide access since they are impersonating a previously verified employee, which makes this a high level of risk.
		7.2) An internal employee loses their work computer. A criminal obtains the computer. The computer is in a locked state.	Confidentiality: A criminal is able to access sensitive information on the work computer by detaching the hard drive and accessing the file system on a separate device.	Risk Level: Medium level of risk for Confidentiality. Justification: This is a medium risk for confidentiality, for the criminal is able to access private information from the work computer. The hard drive, however, must remain intact, and the file system must not be corrupted during this process. The criminal will not be able to modify the information on a system-wide level or make information unavailable.
		7.3) An internal employee's work phone is stolen by a criminal. The phone does not have a password and is not locked. The phone has work	Confidentiality: A criminal is able to access information through the work applications on the phone.	Risk Level: High level of risk for Confidentiality, Integrity, and Availability.

		applications that have active accounts.	Integrity: The criminal is able to impersonate an internal employee and modify system information without having their identity proofed. Availability: The criminal, as an administrator, can revoke access privileges for system information and make information unavailable for all other data owners.	Justification: Since the phone is unlocked and the criminal can easily impersonate an administrator, this is a high level of risk. The criminal is able to access, alter, and transmit information. In addition, they are able to modify the availability of the information for other data owners.
8	Negligence of Personal Information	8.1) An internal employee leaves customer credit card information readily available on his/her computer in the office. The office is robbed, and the criminals take pictures of the information.	Confidentiality: The internal employee left sensitive information open on their computer at work. The criminals were able to access the information and exploit it easily.	Risk Level: Medium level of risk for Confidentiality. Justification: The negligence of the internal employee to hide such information resulted in the violation of confidentiality. The criminals were able to exploit this information for their personal use.
		8.2) An executive officer of Longhorn Ride unintentionally discussed private company information with competing rideshare executives.	Confidentiality: The private company information was leaked by a Longhorn Ride executive. This information may have	Risk Level: Medium level of risk for Confidentiality.

			provided a competitive advantage. It was recorded by competing companies.	Justification: In this instance, the confidentiality of proprietary information was violated. It has a medium level of risk because only the financial valuation of the company was impacted. The other data owners are still protected in this scenario.
9	Lack of Internal Employee Education	9.1) An internal employee opens a spam email from an unidentified source and downloads an attachment with a virus. This virus allows unauthorized access to the employee's personal work device. This can be modified and accessed by the hacker.	Confidentiality: The hacker is able to access and transport information from the internal employee's work device without authorization. Integrity: The hacker is able to modify as well as overwrite data on the internal employee's work device without authorization.	Risk Level: High level of risk for Confidentiality and Integrity. Justification: The hacker is able to access and modify information on the internal employee's computer. They, however, are unable to modify the availability of the information without modifying network privileges directly.
		9.2) Internal employees connect to unsecured Wi-Fi addresses. Device and network information are intercepted by the hackers who have instantiated this dangerous connection.	Confidentiality: Hackers are able to access information transmitted across the network. They are also able to access information on	Risk Level: High level of risk for Confidentiality, Integrity, and Availability.

			the work devices of internal employees. Integrity: Hackers are able to modify information that is transmitted through their dangerous connection. They are able to indirectly modify data elements as well as alter database requests. Availability: The hackers are able to make certain information unavailable to Longhorn Ride administrators connected to their network.	Justification: Hackers are able to access, modify, and regulate the information that internal employees interact with while they are connected to the unsecured Wi-Fi. This allows the criminals to steal and abuse information throughout the entire system.

Risk Impact Estimations:

After identifying the most significant vulnerabilities from the vulnerabilities matrix, we are able to calculate the estimated risk impact for our top two risks. This value reflects the incurred financial losses, damages to the reputation of Longhorn Ride, emotional distress caused to data owners, and inevitable labor costs. These risks are enumerated below.

1) Risk Associated with the OS Command Injection Vulnerability

Every single data element within the data inventory is breached through the network. Since this risk involves compromising all of the data across the entire system (for all data owners), we must calculate the financial loss to be equivalent to the entire valuation of all information associated with Longhorn Ride. This value was calculated to be $140,176,261.70. The estimated time required to address such a gargantuan risk is estimated to be 10,000 hours, for this is the time required to recover such information at this scale. At the rate of $100 per hour, we can calculate labor costs to be $1,000,000. Thus, we can sum the incurred financial losses and the resulting labor costs to determine the risk impact estimation – which is $141,176,261.70. Since all of the data elements within the data inventory are compromised, the reputational damage is high, and the emotional distress caused to data owners is high. All data owners must invest time and money to recover their credentials, replace their PII, and secure their information once again. This results in the highest possible level of distress for all data owners. Additionally, the damage done to the reputation of Longhorn Ride is irreversible; the next steps taken by Longhorn Ride to address the issue and repair relations with stakeholders will define the future of the company.

$$\boxed{\begin{array}{c}\boldsymbol{Risk\ Impact\ Estimation = \$141,176,261.70} \\ \boldsymbol{Damage\ to\ Reputation\ is\ High} \\ \boldsymbol{Emotional\ Distress\ is\ High}\end{array}}$$

2) Risk Associated with the Unsecure Third-Party Cloud-Storage Application

All of the data elements that Longhorn Ride is compromised through the unsecure cloud-storage vendor. Since this risk involves a total breach for every data owner, we must calculate the financial loss to be equivalent to the entire valuation of all information associated with Longhorn Ride. This value was calculated to be $140,176,261.70. The estimated time required to address such a gargantuan risk is estimated to be 500 hours, for the solution is to change cloud-storage providers. At the rate of $100 per hour, we can calculate labor costs to be $50,000. Thus, we can sum the incurred financial losses and the resulting labor costs to determine the risk impact estimation – which is $140,226,261.70. The reputational damage done to Longhorn Ride and the emotional distress caused to data owners by the breach of the entire data inventory is high. The reputation of the company is now permanently defined by the breach in security. The effort, in the context of time and money, exerted by all of the data owners causes a high level of emotional distress, for the process to replace, revalidate, and recover personally identifiable information (PII) is of the highest possible caliber.

$$\boxed{\begin{array}{c} \boldsymbol{Risk\ Impact\ Estimation} = \ \$\mathbf{140,226,261.70} \\ \boldsymbol{Damage\ to\ Reputation\ is\ High} \\ \boldsymbol{Emotional\ Distress\ is\ High} \end{array}}$$

7 Trusted Identity for Information Access and Sharing Controls

7.1 Access Control Design

Our company, Longhorn Ride, implements an Attribute-Based Access Control (ABAC) design. This is an access control design that assesses attributes in order to grant authorization privileges to users. Attributes are classified into three categories: subject attributes, resource attributes, action attributes, and environmental attributes. Subject attributes include information and characteristics about the user that is trying to access and modify data elements within the system. Resource attributes refer to the classifications of the data elements that are being accessed. Action attributes refer to what is being done by the user with the data elements; it includes how the data is accessed and modified. Environmental attributes include contextual information such as location, time, digital method, and security protocols that are associated with the data elements. These attributes can be combined when evaluated in order to create a policy – which grants authorization privileges to users when satisfied. Established policies enable engines to permit or deny authorization and create a standardized security system that protects private information.

Access Control Design: Attribute-Based Access Control (ABAC)

Rationale:

The Attribute-Based Access Control (ABAC) design is the most appropriate access control design for Longhorn Ride because it provides the most security, mitigates risks with its robust structure, and promotes scalability due to its flexible design. It ensures that only the intended parties are able to access and modify sensitive data – which creates a security infrastructure capable of protecting data in each phase of the identity life cycle.

Since the Attribute-Based Access Control (ABAC) methodology evaluates multiple criteria (users, environments, actions, and resources), it is inherently more secure than access control designs that rely on only one. Additionally, users are denied access to resources and data elements unless they are explicitly authorized; this is known as the Fail-Safe Defaults design principle. This ensures that access and modification privileges are granted only when the appropriate user, environment, action, and resource conditions are met. This minimizes the risk of a data breach and ensures that data elements within the information inventory are protected. Information is also secured in each of the phases during the identity lifecycle. There are nine phases: enrollment, identity proofing, authorization, issuance, authentication, use, access and privilege management, storage, and sunsetting. In enrollment, no access to data elements within the data inventory is granted. After the identity proofing phase has been completed and identities have been verified, authorization privileges are granted to identities based on their collected attributes in accordance with established policies. Users will then receive individual tokens and credentials that that allow them to be authenticated by our security systems. If any of these credentials are compromised, all access and modification privileges for data elements will be revoked.

During the sue phase, users must still satisfy the policies in order to access and modify data. Since user, resource, action, and environment attributes change dynamically, these attributes must be checked with the policy each time. The advantage of this access control design is that continual verification ensures the highest level of data security. The tradeoff, however, is that this process will take more time and there will be a greater activity load on the system. We must also restrict access to the privilege management component of our systems in order to ensure that policies are modified by the appropriate individuals. Access and modification to cloud storage elements will also be subject to verification against established policies. Finally, sunsetting protocols will not impact other users and modify the policies. For Longhorn Ride, an Attribute-Based Access Control (ABAC) design is the most appropriate and secure design that protects information in each phase of the identity lifecycle. This allows us to minimize risks, avoid data breaches, and secure sensitive information.

Research Sources:

"Attribute Based Access Control." NIST, https://csrc.nist.gov/Projects/Attribute-Based-Access-Control. Accessed April 9 2020.

"Attribute Based Access Control (ABAC)." Axiomatics, https://www.axiomatics.com/attribute-based-access-control/. Accessed 9 April 2020.

"Role-Based Access Control vs Attribute-Based Access Control: How to Choose." EKRAN, https://www.ekransystem.com/en/blog/rbac-vs-abac. Accessed 9 April 2020.

7.2 Stakeholder Types Requiring Access

Table 6. **Stakeholder Types Requiring Access**

Type of Stakeholder	Description of the Stakeholder
Customer/Rider (External)	Customers/Riders are stakeholders that use the Longhorn Ride rideshare platform in order to travel. After creating an account, customers/riders are able to order a vehicle that will pick them up from a designated location and drop them at their intended destination. Once the ride is completed, these stakeholders will be charged; part of the money goes to the drivers and part of the money goes towards Longhorn Ride. Creating an account requires riders to input personal information in order to be recognized by the drivers. This information is used to complete the identity proofing and authorization phases of the identity life cycle. They can then create a username and password that they will use for authentication I the future. Once in the application, they can input credit card or banking information so that they can be appropriately charged after using the platform to travel; this allows them to then access and interact with driver information on the platform They can also customize ride settings such as enabling disabilities, adding security measures, and setting group sizes – which change their status in the system. Although they are given information access to rider and driver information, they are only able to modify their personal rider data elements.
Driver (External)	Drivers are stakeholders that use the Longhorn Ride platform in order to earn money by giving rides to customers/riders. After creating an account, going through a background check, and verifying their vehicle status, they are able to give rides to nearby customers/riders. They can complete the identity proofing and authorization phases of the identity lifecycle by providing personal information, completing a background check, and proving that their vehicle is appropriate condition. Afterwards they create their username and password credentials in order to be authenticated in future sessions. They are able to access

	the information of drivers and customers. On the other hand, they are only able to modify their own personal information. They are able to access personal customer information per ride in order to identify riders; this information is then cleared once the customers are picked up. They are also able to access modify personal information, driver settings, banking information, and tax information. Additionally, they are able to access certain employee benefits. These data elements will update regularly and be reflected on the databases and rideshare systems.
Investor (External)	Investors are stakeholders that contribute to Longhorn Ride financially in exchange for future return or company shares. After submitting PII and financial information in order to complete the identity proofing stages as well as obtain authorization privileges, they are given credentials that allow them to access proprietary company information. Investors are able to access and modify personal information stored on the system such as banking information and PII. Additionally, they are able to access (but not modify) proprietary data elements pertaining to the business and finances of Longhorn Ride. They are able to access information such as total company valuation, number of users, usage trends over time, share value, return on investment (ROI) data, and budget reports. This allows them to monitor their investment and track the projected performance of Longhorn Ride – which encourages future investment.
Internal Employee – IT Department (Internal)	The internal employees within the IT department are stakeholders that develop, maintain, and contribute to the technological systems that allow the Longhorn Ride platform to function. After getting hired, passing a background check, and completing employment training, the employees of the IT department are able to complete the enrollment, identity proofing, and authorization stages of the identity lifecycle. They then receive credentials that grant them administrator privileges for internal systems and the network. The IT department is able to access and modify data elements within the data inventory, network information,

	database information, and internal system information. They use this information to develop and maintain the Longhorn Ride platform and systems. They configure the security systems, create the user interface, construct the backend, and ensure that the database endpoints are functioning appropriately. Employees are also able to access and modify their own personal information; this includes financial information, tax information, personal compensation plans, and immigration information.
Internal Employee – HR Department (Internal)	The internal employees within the HR department are stakeholders that manage employee, driver, customer/rider, investor, executive, and external information. They ensure that tax, immigration, legal, and compensation processes are appropriately conducted. After getting hired, passing a background check, and completing employment training, the employees of the HR department are able to complete the enrollment as well as identity proofing stages of the identity lifecycle; afterwards, they are granted authorization privileges to the system in order to access and modify stakeholder information. The HR department must access and modify business information within the data inventory in order to ensure that functional business practices occur. They issue tax information (to other employees), handle compensations (for all employees and drivers), pay external entities (such as insurance companies as well as cloud storage vendors), take care of legal procedures, maintain immigration statuses (for all internal employees), and ensure that the company is operating appropriately.
Executive Board of Longhorn Ride (Internal)	The executive board of Longhorn Ride are the stakeholders that are either founders of the company or primary leads for the major divisions within the company. They have the highest level of authorization and associated credentials. This grants them access and modification privileges to all of the data elements within the information inventory. They have access to the most sensitive data and most restricted proprietary information (such as specific sector valuations, future projects, and intellectual property information). They

	are the highest level of the company – which also means they have the highest level of clearance in the implemented security systems.
Third-Party Vendor – Cloud Storage (External)	The third-party cloud storage vendor is a stakeholder that hosts a cloud database that houses all of the Longhorn Ride information in an offsite location. They are able to access and modify database endpoints for security purposes; this includes interrupting connections if the network is compromised as well as preventing digital attacks. They also maintain the database, scale the infrastructure, and provide a security infrastructure (for both the network and the database itself). They do not have access or modification privileges for any of the data elements within the data inventory.
External Entity – Insurance Companies (External)	The insurance companies are stakeholders that are invested on the performance and status of the company. They are external entities that provide protection and compensation for data, financial, and intellectual loss. Longhorn Ride pays insurance companies in order to protect against the repercussions of data breaches and disasters. Insurance companies also provide services that minimize risk and manage potential threats to the company. There are different types of insurance. Longhorn Ride has cyber insurance, disaster insurance, medical insurance, property insurance, and liability insurance. Insurance companies do not have access or modification privileges for any of the data elements within the data inventory because they are an external entity.

7.3 Level of Assurance for Stakeholder Authentication

Table 7. **Stakeholder Authentication – Levels of Assurance**

Type of Stakeholder	Classification for Information Assessed	Identity Assurance Level (IAL)	Token Assurance Level (TAL)	Level of Assurance (LOA) (Levels 1 – 4)	Justification for Assignment of Assurance Levels
Customer/Rider	Public	Low	Low	Level 1	Customer/Riders are assigned a low Identity Assurance Level (IAL) because they have public data that is fluid in nature. Thus, they are issued a low degree of confidence for who they claim to be for IAL. They are also assigned a low Token Assurance Level (TAL) because customers are prone to losing login information and assigned credentials for public and low value data. Thus, they are issued a low degree of confidence for maintaining their associated tokens. They are assigned a Level 1 for their Level of Assurance because there is no identity proofing required. These assurance levels for customers/riders and their public data allow for high customer convenience, reasonable security, and lowered costs for the company.

Customer/Rider	Proprietary	Medium	Low	Level 2	Customer/Riders are assigned a medium Identity Assurance Level (IAL) because they have proprietary data that should be kept private in order for Longhorn Ride to maintain a competitive advantage over other rideshare companies. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a low Token Assurance Level (TAL) because customers are prone to losing login information and assigned credentials for proprietary data that does not directly concern them. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 2 for their Level of Assurance because they require single-factor authentication and identity proofing for this information. These assurance levels for customers/riders and their proprietary data allow for high rider convenience,

					reasonable security, and lowered company costs.
Customer/Rider	Confidential	Medium	Medium	Level 3	Customer/Riders are assigned a medium Identity Assurance Level (IAL) because they have confidential data that they would not like disclosed. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a medium Token Assurance Level (TAL) because customers reasonably maintain tokens associated with their personal private information. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because they require multi-factor authentication and identity proofing for this information. These assurance levels for customers/riders and their confidential data allow for reasonable rider convenience, higher security, and reasonable company costs.
Customer/Rider	Regulatory	Medium	High	Level 3	Customer/Riders are assigned a medium

					Identity Assurance Level (IAL) because they have regulatory data that is highly sensitive; such information should be kept private in order to minimize risks and losses. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because customers usually maintain tokens associated with their most sensitive information quite well. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because they require multi-factor authentication and identity proofing for this information. These assurance levels for customers/riders and their regulatory data allow for reasonable rider convenience, the highest level of security, reasonable company costs, and the highest level of privacy.

Driver	Public	Low	Low	Level 2	Drivers are assigned a low Identity Assurance Level (IAL) because they have public data that is fluid in nature. Thus, they are issued a low degree of confidence for who they claim to be for IAL. They are also assigned a low Token Assurance Level (TAL) because drivers are prone to losing login information and assigned credentials for public and data that is low in value. Thus, they are issued a low degree of confidence for maintaining their associated tokens. They are assigned a Level 2 for their Level of Assurance because employed driver must go through at least a single-factor authentication and identity proofing. These assurance levels for drivers and their public data allow for high driver convenience, reasonable security, and lowered costs for the company.
Driver	Proprietary	Medium	Medium	Level 2	Drivers are assigned a medium Identity Assurance Level (IAL) because they have proprietary data that

					should be kept private in order for Longhorn Ride to maintain a competitive advantage over other rideshare companies. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a medium Token Assurance Level (TAL) because drivers are not as concerned with proprietary data. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 2 for their Level of Assurance because they require single-factor authentication and identity proofing for this information. These assurance levels for drivers and their proprietary data allow for high driver convenience, reasonable security, and lowered company costs.
Driver	Confidential	Medium	Medium	Level 3	Drivers are assigned a medium Identity Assurance Level (IAL) because they have confidential data that they would not like disclosed. Thus, they are

					issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a medium Token Assurance Level (TAL) because drivers appropriately maintain tokens associated with their personal and private information. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because they require multi-factor authentication and identity proofing for this information. These assurance levels for drivers and their confidential data allow for reasonable driver convenience, higher security, and reasonable company costs.
Driver	Regulatory	High	High	Level 4	Drivers are assigned a high Identity Assurance Level (IAL) because they have regulatory data that is highly sensitive; such information should be kept private in order to minimize risks and losses (for both the driver and for Longhorn Ride). Thus, they are

					issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because customers usually maintain tokens associated with their most sensitive information quite well. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for drivers and their regulatory data allow for reasonable driver convenience, the highest level of security, reasonable company costs, and the highest level of privacy.
Investor	Public	Low	Medium	Level 2	Investors are assigned a low Identity Assurance Level (IAL) because they have public data that is fluid in nature. Thus, they are issued a low degree of confidence for who they claim to be for

					IAL. They are also assigned a medium Token Assurance Level (TAL) because investors reasonably maintain their credentials associated with lower valued data. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 2 for their Level of Assurance because investors must go through at least a single-factor authentication and identity proofing. These assurance levels for investors and their public data allow for high convenience, reasonable security, and lowered costs for the company.
Investor	Proprietary	Medium	High	Level 3	Investors are assigned a medium Identity Assurance Level (IAL) because they have proprietary data that should be kept private in order for Longhorn Ride to maintain a competitive advantage over other rideshare companies. By protecting proprietary data, they are also protecting their investments. Thus, they

					are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because investors will maintain and protect credentials associated with business and investment information. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because they require multi-factor authentication and identity proofing for this information. These assurance levels for investors and their proprietary data allow for reasonable investor convenience, high security, and reasonable company costs.
Investor	Confidential	High	High	Level 4	Investors are assigned a high Identity Assurance Level (IAL) because they have confidential data that they would not like released. Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level

					(TAL) because investors take great care of credentials associated with their investment data. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for investors and their confidential data allow for reasonable investor convenience, higher security, and reasonable company costs.
Investor	Regulatory	High	High	Level 4	Investors are assigned a high Identity Assurance Level (IAL) because they have regulatory data that is highly sensitive; such information should be kept private in order to minimize risks and losses (for both the investors and for Longhorn Ride). Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because investors take

					great care of credentials associated with their investment data. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for investors and their regulatory data allow for reasonable investor convenience and reasonable company costs. They focus more on ensuring the highest level of security and privacy.
Internal Employee (IT Department)	Public	Medium	Medium	Level 3	Internal employees within the IT department are assigned a medium Identity Assurance Level (IAL) because they have public data that can be shared as long as it is appropriately maintained. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a medium Token Assurance Level

					(TAL) because employees reasonably maintain their credentials associated with lower valued data. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because employees must go through multi-factor authentication process and identity proofing. These assurance levels for employees and their public data allow for high convenience, reasonable security, and lowered costs for the company.
Internal Employee (IT Department)	Proprietary	Medium	High	Level 4	Internal employees within the IT department are assigned a medium Identity Assurance Level (IAL) because they have proprietary data that should be kept private in order for Longhorn Ride to maintain a competitive advantage over other rideshare companies. By protecting proprietary data, they are also protecting their own projects and work. Thus,

					they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because employees will maintain and protect credentials associated with business information and personal work. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing before they can access and modify this type of information. These assurance levels for employees and their proprietary data allow for reasonable employee convenience, high security, and reasonable company costs.
Internal Employee (IT Department)	Confidential	High	High	Level 4	Internal employees within the IT department are assigned a high Identity Assurance Level (IAL) because they have confidential data that they would not like

					released. Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because employees take great care of credentials associated with personal work and business-related data. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for employees and their confidential data allow for reasonable employee convenience, higher security, and reasonable company costs.
Internal Employee (IT Department)	Regulatory	High	High	Level 4	Internal employees within the IT department are assigned a high Identity Assurance Level (IAL) because they have regulatory data that is highly sensitive; such information should be

					kept private in order to minimize risks and losses (for both the employees and for Longhorn Ride). Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because employees must maintain and protect high-profile data associated with internal systems. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for employees and their regulatory data allow for reasonable employee convenience and reasonable company costs. Comparatively, a stronger emphasis is placed on ensuring the highest level of security and privacy.

Internal Employee (HR Department)	Public	Medium	Medium	Level 3	Internal employees within the HR department are assigned a medium Identity Assurance Level (IAL) because they have public data that can be shared as long as it is appropriately maintained. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a medium Token Assurance Level (TAL) because employees reasonably maintain their credentials associated with lower valued data. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because employees must go through multi-factor authentication process and identity proofing. These assurance levels for employees and their public data allow for high convenience, reasonable security, and lowered costs for the company.

Internal Employee (HR Department)	Proprietary	Medium	High	Level 4	Internal employees within the HR department are assigned a medium Identity Assurance Level (IAL) because they have proprietary data that should be kept private in order for Longhorn Ride to maintain a competitive advantage over other rideshare companies. By protecting proprietary data, they are also protecting their own projects and work. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because employees will maintain and protect credentials associated with business information and personal work. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing before they can access and modify this type of

					information. These assurance levels for employees and their proprietary data allow for reasonable employee convenience, high security, and reasonable company costs.
Internal Employee (HR Department)	Confidential	High	High	Level 4	Internal employees within the HR department are assigned a high Identity Assurance Level (IAL) because they have confidential data that they would not like released. Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because employees take great care of credentials associated with personal work and business-related data. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information.

					These assurance levels for employees and their confidential data allow for reasonable employee convenience, higher security, and reasonable company costs.
Internal Employee (HR Department)	Regulatory	High	High	Level 4	Internal employees within the HR department are assigned a high Identity Assurance Level (IAL) because they have regulatory data that is highly sensitive; such information should be kept private in order to minimize risks and losses (for both the employees and for Longhorn Ride). Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because employees must maintain and protect high-profile data associated with related business procedures. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they

					require multi-factor authentication and in-person identity proofing for this information. These assurance levels for employees and their regulatory data allow for reasonable employee convenience and reasonable company costs. Comparatively, a stronger emphasis is placed on ensuring the highest level of security and privacy.
Executive Board of Longhorn Ride	Public	Medium	Medium	Level 3	The executive board members of Longhorn Ride are assigned a medium Identity Assurance Level (IAL) because they have public data that can be shared as long as it is appropriately maintained. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a medium Token Assurance Level (TAL) because executive members reasonably maintain their credentials associated with lower valued data. Thus, they are issued a medium degree of confidence for

					maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because executives must go through multi-factor authentication process and identity proofing. These assurance levels for employees and their public data allow for high convenience, reasonable security, and lowered costs for the company.
Executive Board of Longhorn Ride	Proprietary	High	High	Level 4	The executive board members of Longhorn Ride are assigned a high Identity Assurance Level (IAL) because they have authorization privileges to access and modify extremely sensitive proprietary data. This data should be kept private in order for Longhorn Ride to maintain a competitive advantage over other rideshare companies. By protecting proprietary data, they are also protecting their own data and company. Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level

					(TAL) because executive members will maintain and protect credentials associated with business information and internal systems. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing before they can access and modify this type of information. These assurance levels for executives and their proprietary data allow for a high level of privacy and security in exchange for reduced convenience (for executive members).
Executive Board of Longhorn Ride	Confidential	High	High	Level 4	The executive board members of Longhorn Ride are assigned a high Identity Assurance Level (IAL) because they have confidential data that they would not like released. Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because executive

					members take great care of credentials associated with personal work and business-related data. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for executives and their confidential data allow for reasonable employee convenience, higher security, and reasonable company costs.
Executive Board of Longhorn Ride	Regulatory	High	High	Level 4	The executive board members of Longhorn Ride are assigned a high Identity Assurance Level (IAL) because they have regulatory data that is extremely sensitive; such information should be kept private in order to minimize risks and losses (for both the executives and for Longhorn Ride). Thus, they are issued a high degree of confidence for who they claim to be for

					IAL. They are also assigned a high Token Assurance Level (TAL) because executive members must maintain and protect high-profile data associated with related business procedures. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing to access and modify such information. These assurance levels for executives and their regulatory data reduce executive convenience and increase company costs for security systems. In the long run, however, security and privacy are maximized.
Third-Party Vendor – Cloud Storage	Public	Low	Medium	Level 3	Third-party cloud storage vendors are assigned a low Identity Assurance Level (IAL) because they have public data that can be shared, for it is the basis of their business. Thus, they are issued a low degree of confidence for

					who they claim to be for IAL. They are also assigned a medium Token Assurance Level (TAL) because third-party cloud storage vendors will reasonably maintain their credentials associated with lower valued data so that they can protect their own data inventory. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because third-party vendors must go through multi-factor authentication process and identity proofing. These assurance levels for third-party cloud storage vendors and their public data allow for high convenience, reasonable security, and lowered costs for the companies involved (Longhorn Ride and the cloud storage vendor).
Third-Party Vendor – Cloud Storage	Proprietary	Medium	High	Level 3	Third-party cloud storage vendors are assigned a medium Identity Assurance Level (IAL) because they have limited privileges to

					access proprietary data. They are only able to access proprietary data that pertains to cloud storage and database usage. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because third-party cloud storage vendors will maintain and protect their credentials because they directly affect their own business as well as internal procedures. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because they require multi-factor authentication and identity proofing before they can access and modify this type of information. These assurance levels for third-party cloud storage vendors and their proprietary data allow for high convenience, reasonable security, and

					lowered costs for the companies involved (Longhorn Ride and the cloud storage vendor).
Third-Party Vendor – Cloud Storage	Confidential	High	High	Level 4	Third-party cloud storage vendors are assigned a high Identity Assurance Level (IAL) because they have confidential data that they would not like released. Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because third-party vendors protect their clients' credentials since it directly impacts their business. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for third-party cloud storage vendors and their confidential data allow for the highest level of security, reasonable convenience, and

					lowered costs (for Longhorn Ride and the cloud storage vendor).
Third-Party Vendor – Cloud Storage	Regulatory	High	High	Level 4	Third-party cloud storage vendors are assigned a high Identity Assurance Level (IAL) because they have regulatory data that is extremely sensitive; such information should be kept private in order to minimize risks and losses (for both the third-party vendor and for Longhorn Ride). Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because third-party cloud storage vendors protect their clients' credentials since it directly impacts their business. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing to access and modify such information. These assurance levels for

					third-party cloud storage vendors and their regulatory data reduce overall convenience and increase company costs for security systems. In the long run, however, security and privacy are maximized – which protects both the data inventory of both companies.
External Entity – Insurance Companies	Public	Low	Medium	Level 3	Insurance companies are assigned a low Identity Assurance Level (IAL) because they have public data that must be shared in order for their business to function appropriately. Thus, they are issued a low degree of confidence for who they claim to be for IAL. They are also assigned a medium Token Assurance Level (TAL) because insurance companies will reasonably maintain their credentials associated with lower valued data so that they can protect their own data inventory. Thus, they are issued a medium degree of confidence for maintaining their associated tokens. They

					are assigned a Level 3 for their Level of Assurance because third-party vendors must go through multi-factor authentication process and identity proofing. These assurance levels for insurance companies and their public data allow for high convenience, reasonable security, and lowered costs for the companies involved (Longhorn Ride and the insurance company).
External Entity – Insurance Companies	Proprietary	Medium	High	Level 3	Insurance companies are assigned a medium Identity Assurance Level (IAL) because they have limited privileges to access proprietary data. They are only able to access proprietary data that pertains to Longhorn Ride insurance policies. Thus, they are issued a medium degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because insurance companies will maintain and protect their credentials because they directly affect their insurance business.

					Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 3 for their Level of Assurance because they require multi-factor authentication and identity proofing before they can access and modify this type of information. These assurance levels for insurance companies and their proprietary data allow for high convenience, reasonable security, and lowered costs for the companies involved (Longhorn Ride and the insurance companies).
External Entity – Insurance Companies	Confidential	High	High	Level 4	Insurance companies are assigned a high Identity Assurance Level (IAL) because they have confidential data that they would not like released. Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because insurance companies protect their clients' credentials since it directly impacts their business. Thus, they are

					issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing for this information. These assurance levels for insurance companies and their confidential data allow for the highest level of security, reasonable convenience, and lowered costs (for Longhorn Ride and the insurance company).
External Entity – Insurance Companies	Regulatory	High	High	Level 4	Insurance companies are assigned a high Identity Assurance Level (IAL) because they have regulatory data that is extremely sensitive; such information should be kept private in order to mitigate threats and losses (for both the insurance company and for Longhorn Ride). Thus, they are issued a high degree of confidence for who they claim to be for IAL. They are also assigned a high Token Assurance Level (TAL) because insurance companies are required

					legally to protect their clients’ credentials. Additionally, maintaining their clients’ credentials directly impacts their business. Thus, they are issued a high degree of confidence for maintaining their associated tokens. They are assigned a Level 4 for their Level of Assurance because they require multi-factor authentication and in-person identity proofing to access and modify such information. These assurance levels for insurance companies and their regulatory data reduce overall convenience and increase company costs for security systems. In the long run, however, security and privacy are maximized – which protects both the data inventory of both companies.

7.4 Stakeholder Access Control

Table 8. **Access Controls for Stakeholders**

Type of Stakeholder	Access Control Specification	Access Control Specification Applies to What Data Elements of the Information Inventory
Customer/Rider (Public Data Elements)	IF {((Subject == Customer/Rider) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Resource == Public Data Element) AND (Action == Access OR Modify))	Rider Name, Rider Phone Number, Rider Email Address, Rider Disability Status, Rider Ride rating, Rider Gender, Rider Account Picture, Rider Promotional Codes
Customer/Rider (Proprietary Data Elements)	IF {((Subject == Customer/Rider) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Proprietary Data Element) AND (Action == Access OR Modify))	Rider Ride History, Rider Rideshare Call History, Rider Number of Cancellations, Rider Pet Information, Rider Party Size, Rider Conversation Preference, Rider Smoking Preference, Rider Carpool Preference, Rider Language Preference, Rider Rideshare Messages
Customer/Rider (Confidential Data Elements)	IF {((Subject == Customer/Rider) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data Element) AND (Action == Access OR Modify))	Rider Address, Rider Age, Rider Date of Birth, Rider Username, Rider Password, Rider Emergency Contact Information, Ride Account Security Questions, Rider Billing Address, Rider Pick-Up Location, Rider Destination, Rider Zip Code, Rider Height, Rider Weight, Rider Ethnicity, Rider Allergies
Customer/Rider (Regulatory Data Elements)	IF {((Subject == Customer/Rider) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (Token == Multi-Factor One-Time Password (OTP))	Rider Credit Card Information, Rider Bank Account Routing Information, Rider Current Location

	AND (Resource == Regulatory Data Element) AND (Action == Access OR Modify))	
Driver (Public Data Elements)	IF {((Subject == Driver) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Resource == Public Data Element) AND (Action == Access OR Modify))	Driver Name, Driver Phone Number, Driver Email Address, Driver Ride Rating, Driver Gender, Driver Account Picture, Driver Vehicle License Plate Number, Driver Vehicle Color, Driver Vehicle Model, Driver Vehicle Pet Accommodation
Driver (Proprietary Data Elements)	IF {((Subject == Driver) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Proprietary Data Element) AND (Action == Access OR Modify))	Driver Ride History, Driver Rideshare Call History, Driver Active Status, Driver Number of Cancellations, Driver Work Time Sheet, Driver Conversation Preferences, Driver Driving Distance Preferences, Driver Smoking Preferences, Driver Language Preferences, Driver Number of Proficient Languages, Driver Rideshare Messages, Driver Employment Start Date, Driver Vehicle insurance, Driver Vehicle Disability Accommodation, Driver Vehicle Maximum Capacity, Driver Vehicle Luggage Capacity, Driver Vehicle Bluetooth Compatibility, Driver Vehicle Self-Driving Capability, Driver Vehicle Electric/Hybrid Automobile Classification, Driver Vehicle Height Clearance, Driver Vehicle Texas registration Status, Driver Vehicle Inspection Status
Driver (Confidential Data Elements)	IF {((Subject == Driver) AND (UsernameCredential == Username) AND (PasswordCredential ==	Driver Address, Driver Age, Driver Date of Birth, Driver Username, Driver password,

	Password) AND (EmailCredential == Email Address) AND (DriverCredential == Driver's License) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data Element) AND (Action == Access OR Modify))	Driver Current Location, Driver Emergency Contact Information, Driver Account Security Questions, Driver Billing Address, Driver Criminal History, Driver Medical History, Driver Employment History, Driver Veteran Status, Driver Citizenship Status, Driver, Driver's License Number, Driver Accident History, Driver Zip Code, Driver Height, Driver Weight, Driver Ethnicity, Driver Allergies
Driver (Regulatory Data Elements)	IF {((Subject == Driver) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (DriverCredential == Driver's License) AND (Token == Multi-Factor One-Time Password (OTP)) AND (Resource == Regulatory Data Element) AND (Action == Access OR Modify))	Driver Credit Card Information, Driver Bank Account Routing Information, Driver Social Security Number, Driver Work Authorization Status, Driver Employment Eligibility Verification (I-9), Driver Employee Identification Number (EIN), Driver Tax Form W-2, Driver Tax Form W-4, Driver Rideshare Insurance, Driver Vehicle Toll Tag Number
Investor (Public Data Elements)	IF {((Subject == Investor) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Resource == Public Data Element) AND (Action == Access OR Modify))	Longhorn Ride Company Net Worth, Longhorn Ride Company Official Address (Headquarters)
Investor (Proprietary Data Elements)	IF {((Subject == Investor) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource ==	Investor Name, Investor Phone Number, Investor Email Address, Investor Relation to Longhorn Ride Company, Investor Investment Date

	Proprietary Data Element) AND (Action == Access OR Modify))	
Investor (Confidential Data Elements)	IF {((Subject == Investor) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (InvestorIDCredential == Investor ID) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data Element) AND (Action == Access OR Modify))	Investor Address, Investor Occupation, Investor Return on Investment Value
Investor (Regulatory Data Elements)	IF {((Subject == Investor) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (EmailCredential == Email Address) AND (InvestorIDCredential == Investor ID) AND (Token == Multi-Factor One-Time Password (OTP)) AND (Resource == Regulatory Data Element) AND (Action == Access OR Modify))	Investor Bank Account Routing Information, Investor Total Equity/Stock Value
Internal Employee – **IT Department** (Public Data Elements)	IF {((Subject == Employee) AND (Employee Type = IT) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Resource == Public Data Element) AND (Action == Access OR Modify))	Employee Name, Employee Phone Number, Employee Email Address, Employee Job Title, Driver Name, Driver Phone Number, Driver Email Address, Driver Ride Rating, Driver Gender, Driver Account Picture, Driver Vehicle License Plate Number, Driver Vehicle Color, Driver Vehicle Model, Driver Vehicle Pet Accommodation, Rider Name, Rider Phone Number, Rider Email Address, Rider Disability Status, Rider Ride rating, Rider Gender, Rider Account Picture, Rider

		Promotional Codes, Longhorn Ride Company Net Worth, Longhorn Ride Company Official Address (Headquarters), Longhorn Ride Company Number of Office Locations, Longhorn Ride Company Website Domain Name
Internal Employee – IT Department (Proprietary Data Elements)	IF {((Subject == Employee) AND (Employee Type = IT) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Proprietary Data Element) AND (Action == Access OR Modify))	Employee Number of Proficient Languages, Employee Employment Start Date, Employee Paid Time Off Amount, Investor Name, Investor Phone Number, Investor Email Address, Investor Relation to Longhorn Ride Company, Investor Investment Date, Driver Ride History, Driver Rideshare Call History, Driver Active Status, Driver Number of Cancellations, Driver Conversation Preferences, Driver Driving Distance Preferences, Driver Smoking Preferences, Driver Language Preferences, Driver Number of Proficient Languages, Driver Rideshare Messages, Driver Vehicle insurance, Driver Vehicle Disability Accommodation, Driver Vehicle Maximum Capacity, Driver Vehicle Luggage Capacity, Driver Vehicle Bluetooth Compatibility, Driver Vehicle Self-Driving Capability, Driver Vehicle Electric/Hybrid Automobile Classification, Driver Vehicle Height Clearance, Driver Vehicle Texas registration Status, Driver Vehicle Inspection Status, Rider

		Ride History, Rider Rideshare Call History, Rider Number of Cancellations, Rider Pet Information, Rider Party Size, Rider Conversation Preference, Rider Smoking Preference, Rider Carpool Preference, Rider Language Preference, Rider Rideshare Messages, Longhorn Ride Company Internal Filing Space Capacity (Physical), Longhorn Ride Company Number of iOS Application Downloads, Longhorn Ride Company Number of Android Application Downloads, Longhorn Ride Company Annual Cost of Hosting Application on iOS Store, Longhorn Ride Company Annual Cost of Hosting Application on Android Store, Longhorn Ride Company Number of Registered Customers/Riders, Longhorn Ride Company Number of Registered Drivers, Longhorn Ride Company Number of Employees, Potential Investor Names, Potential Investor Relation to Longhorn Ride Company, Potential Investor Phone Number, Potential Investor Email Address, Longhorn Ride Company Number of Investors, Longhorn Ride Company Yearly Revenue, Longhorn Ride Company Estimated Market Share Value for Rideshare Service

Internal Employee – **IT Department** (Confidential Data Elements)	IF {((Subject == Employee) AND (Employee Type = IT) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Clearance == Security Clearance OR Government Clearance) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data Element) AND (Action == Access OR Modify))	Employee Address, Employee Age, Employee Date of Birth, Employee Disability Status, Employee Username, Employee Password, Employee Citizenship Status, Employee Driver's License Number, Employee Gender, Employee Emergency Contact Information, Employee Account Security Questions, Employee Account Picture, Employee Billing Address, Employee Criminal History, Employee Life Insurance, Employee Medical History, Employee Employment History, Employee Veteran Status, Employee Salary, Employee Work Time Sheet, Employee Education History, Employee Zip Code, Employee Medical Insurance, Employee Height, Employee Weight, Employee Ethnicity, Employee Allergies, Employee Blood Type, Employee Resume/CV, Employee Number of Dependents (Spouses and Children), Employee Household Income, Employee Location of Permanent Residence, Investor Address, Investor Occupation, Investor Return on Investment Value, Driver Address, Driver Age, Driver Date of Birth, Driver Username, Driver password, Driver Current Location, Driver Emergency Contact Information, Driver Account Security Questions, Driver Billing Address, Driver's License

		Number, Driver Accident History, Driver Zip Code, Driver Height, Driver Weight, Driver Ethnicity, Driver Allergies, Rider Address, Rider Age, Rider Date of Birth, Rider Username, Rider Password, Rider Emergency Contact Information, Ride Account Security Questions, Rider Billing Address, Rider Pick-Up Location, Rider Destination, Rider Zip Code, Rider Height, Rider Weight, Rider Ethnicity, Rider Allergies, Longhorn Ride Company Number of Employee Computers, Total Investment Contributions, Potential Investor Address, Potential Investor Occupation,
Internal Employee – **IT Department** (Regulatory Data Elements)	IF {((Subject == Employee) AND (Employee Type = IT) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Clearance == Security Clearance OR Government Clearance) AND (Token == Multi-Factor One-Time Password (OTP)) AND (Resource == Regulatory Data Element) AND (Action == Access OR Modify))	Employee Credit Card Information, Employee Work Authorization Status, Employee Bank Account Routing Information, Employee 401(k) Information, Employee Social Security Number, Employee Tax Form W-2, Employee Tax Form W-4, Employee Employment Eligibility Verification (I-9), Employee's Employee Identification Number (EIN), Employee Workspace Access Information, Employee Security Clearance (Internal for Company Use), Employee Government Clearance (Government Related Projects), Employee Visa Type, Investor Bank Account Routing Information, Investor Total Equity/Stock Value, Driver

		Credit Card Information, Driver Bank Account Routing Information, Driver Employment, Rider Credit Card Information, Rider Bank Account Routing Information, Rider Current Location, Longhorn Ride Company Employee Computer Identification Numbers, Longhorn Ride Company iOS Application Identification Number, Longhorn Ride Company Android Application Identification Number, Paid Investments (Assets), Unpaid Investments (Liabilities), Longhorn Ride Company Tax Identification Number, Longhorn Ride Company Liability Insurance, Longhorn Ride Company Stock Value, Longhorn Ride Company Number of Office Locations
Internal Employee – HR Department (Public Data Elements)	IF {((Subject == Employee) AND (Employee Type = HR) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Resource == Public Data Element) AND (Action == Access OR Modify))	Employee Name, Employee Phone Number, Employee Email Address, Employee Job Title, Longhorn Ride Company Official Address (Headquarters), Longhorn Ride Company Net Worth, Longhorn Ride Company Website Domain Name
Internal Employee – HR Department (Proprietary Data Elements)	IF {((Subject == Employee) AND (Employee Type = HR) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Token == Single-Factor One-Time Password (OTP)) AND	Longhorn Ride Company Number of Registered Customers/Riders, Longhorn Ride Company Number of Employees, Employee Number of Proficient Languages, Employee Employment Start Date, Employee Paid Time Off

	(Resource == Proprietary Data Element) AND (Action == Access OR Modify))	Amount, Driver Work Time Sheet, Driver Employment Start Date, Third-Party Cloud Storage Vendor Contract Length, Third-Party Cloud Storage Vendor Annual Cost
Internal Employee – HR Department (Confidential Data Elements)	IF {((Subject == Employee) AND (Employee Type = HR) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Clearance == Security Clearance OR Government Clearance) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data Element) AND (Action == Access OR Modify))	Employee Address, Employee Age, Employee Date of Birth, Employee Disability Status, Employee Username, Employee Password, Employee Citizenship Status, Employee Driver's License Number, Employee Gender, Employee Emergency Contact Information, Employee Account Security Questions, Employee Account Picture, Employee Billing Address, Employee Criminal History, Employee Life Insurance, Employee Medical History, Employee Employment History, Employee Veteran Status, Employee Salary, Employee Work Time Sheet, Employee Education History, Employee Zip Code, Employee Medical Insurance, Employee Height, Employee Weight, Employee Ethnicity, Employee Allergies, Employee Blood Type, Employee Resume/CV, Employee Number of Dependents (Spouses and Children), Employee Household Income, Employee Location of Permanent Residence, Driver Criminal History, Driver Medical History, Driver Employment History, Driver Veteran Status, Driver Citizenship Status,

Internal Employee – HR Department (Regulatory Data Elements)	IF {((Subject == Employee) AND (Employee Type = HR) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Clearance == Security Clearance OR Government Clearance) AND (Token == Multi-Factor One-Time Password (OTP)) AND (Resource == Regulatory Data Element) AND (Action == Access OR Modify))	Longhorn Ride Company Tax Identification Number, Longhorn Ride Company Liability Insurance, Longhorn Ride Company Number of Office Locations, Employee Credit Card Information, Employee Work Authorization Status, Employee Bank Account Routing Information, Employee 401(k) Information, Employee Social Security Number, Employee Tax Form W-2, Employee Tax Form W-4, Employee Employment Eligibility Verification (I-9), Employee's Employee Identification Number (EIN), Employee Workspace Access Information, Employee Security Clearance (Internal for Company Use), Employee Government Clearance (Government Related Projects), Employee Visa Type, Driver Social Security Number, Driver Work Authorization Status, Eligibility Verification (I-9), Driver Employee Identification Number (EIN), Driver Tax Form W-2, Driver Tax Form W-4, Driver Rideshare Insurance, Driver Vehicle Toll Tag Number,
Executive Board of Longhorn Ride (Public Data Elements)	IF {((Subject == Employee) AND (Employee Type = Executive) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Resource == Public Data Element) AND (Action == Access OR Modify))	Longhorn Ride Company Net Worth, Longhorn Ride Company Official Address (Headquarters), Longhorn Ride Company Number of Office Locations, Longhorn Ride Company Website Domain Name, Employee Name, Employee

		Phone Number, Employee Email Address, Employee Job Title
Executive Board of Longhorn Ride (Proprietary Data Elements)	IF {((Subject == Employee) AND (Employee Type = Executive) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Proprietary Data Element) AND (Action == Access OR Modify))	Longhorn Ride Company Number of Registered Customers/Riders, Longhorn Ride Company Number of Registered Drivers, Longhorn Ride Company Number of Employees, Potential Investor Names, Potential Investor Relation to Longhorn Ride Company, Potential Investor Phone Number, Potential Investor Email Address, Longhorn Ride Company Number of Investors, Longhorn Ride Company Yearly Revenue, Longhorn Ride Company Estimated Market Share Value for Rideshare Service, Employee Number of Proficient Languages, Employee Employment Start Date, Employee Paid Time Off Amount, Potential Investor Names, Potential Investor Relation to Longhorn Ride Company, Potential Investor Phone Number, Potential Investor Email Address
Executive Board of Longhorn Ride (Confidential Data Elements)	IF {((Subject == Employee) AND (Employee Type = Executive) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Clearance == Security Clearance OR Government Clearance) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data	Total Investment Contributions, Potential Investor Address, Potential Investor Occupation, Employee Address, Employee Age, Employee Date of Birth, Employee Disability Status, Employee Username, Employee Password, Employee Citizenship Status, Employee Driver’s License Number, Employee Gender, Employee Emergency

	Element) AND (Action == Access OR Modify))	Contact Information, Employee Account Security Questions, Employee Account Picture, Employee Billing Address, Employee Criminal History, Employee Life Insurance, Employee Medical History, Employee Employment History, Employee Veteran Status, Employee Salary, Employee Work Time Sheet, Employee Education History, Employee Zip Code, Employee Medical Insurance, Employee Height, Employee Weight, Employee Ethnicity, Employee Allergies, Employee Blood Type, Employee Resume/CV, Employee Number of Dependents (Spouses and Children), Employee Household Income, Employee Location of Permanent Residence
Executive Board of Longhorn Ride (Regulatory Data Elements)	IF {((Subject == Employee) AND (Employee Type = Executive) AND (UsernameCredential == Username) AND (PasswordCredential == Password) AND (Employee ID == Employee Identification Number (EIN)) AND (Clearance == Security Clearance OR Government Clearance) AND (Token == Multi-Factor One-Time Password (OTP)) AND (Resource == Regulatory Data Element) AND (Action == Access OR Modify))	Paid Investments (Assets), Unpaid Investments (Liabilities), Longhorn Ride Company Tax Identification Number, Longhorn Ride Company Liability Insurance, Longhorn Ride Company Stock Value, Longhorn Ride Company Number of Office Locations, Employee Credit Card Information, Employee Work Authorization Status, Employee Bank Account Routing Information, Employee 401(k) Information, Employee Social Security Number, Employee Tax Form W-2, Employee Tax Form W-4, Employee Employment

		Eligibility Verification (I-9), Employee’s Employee Identification Number (EIN), Employee Workspace Access Information, Employee Security Clearance (Internal for Company Use), Employee Government Clearance (Government Related Projects), Employee Visa Type
Third-Party Vendor – Cloud Storage (Public Data Elements)	IF {((Subject == Third-Party Vendor) AND (Service Type == Cloud Storage) AND (Service ID == Cloud Service Identification Number) AND (Resource == Public Data Element) AND (Action == Access))	Longhorn Ride Company Number of Office Locations, Longhorn Ride Company Website Domain Name
Third-Party Vendor – Cloud Storage (Proprietary Data Elements)	IF {((Subject == Third-Party Vendor) AND (Service Type == Cloud Storage) AND (Service ID == Cloud Service Identification Number) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Proprietary Data Element) AND (Action == Access))	Longhorn Ride Company Internal Server Space/Memory Capacity (Digital), Longhorn Ride Company Website Traffic Value, Longhorn Ride Company Number of Transactions on Website, Longhorn Ride Company Number of Transactions on iOS Application, Longhorn Ride Company Number of Transactions on Android Application, Third-Party Cloud Storage Vendor Name, Third-Party Cloud Storage Vendor Storage/Memory Capacity, Third-Party Cloud Storage Vendor Contract Length, Third-Party Cloud Storage Vendor Annual Cost, Third-Party Cloud Storage Vendor Bandwidth
Third-Party Vendor – Cloud Storage (Confidential Data Elements)	IF {((Subject == Third-Party Vendor) AND (Service Type == Cloud Storage) AND (Service ID == Cloud	Longhorn Ride Company Number of Employee Computers, Total Investment

	Service Identification Number) AND (Session ID = Specific Session Number) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data Element) AND (Action == Access))	Contributions, Longhorn Ride Company Number of Employee Computers
Third-Party Vendor – Cloud Storage (Regulatory Data Elements)	IF {((Subject == Third-Party Vendor) AND (Service Type == Cloud Storage) AND (Service ID == Cloud Service Identification Number) AND (Session ID = Specific Session Number) AND (Token == Multi-Factor One-Time Password (OTP)) AND (Resource == Public Data Element) AND (Action == Access))	Longhorn Ride Company iOS Application Identification Number, Longhorn Ride Company Android Application Identification Number, Longhorn Ride Company Annual Cost of Hosting Application on iOS Store, Longhorn Ride Company Annual Cost of Hosting Application on Android Store
External Entity – Insurance Companies (Public Data Elements)	IF {((Subject == External Entity) AND (Service Type == Insurance) AND (Service ID == Insurance Identification Number) AND (Resource == Public Data Element) AND (Action == Access))	Longhorn Ride Company Number of Office Locations
External Entity – Insurance Companies (Proprietary Data Elements)	IF {((Subject == External Entity) AND (Service Type == Insurance) AND (Service ID == Insurance Identification Number) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Proprietary Data Element) AND (Action == Access))	Longhorn Ride Company Estimated Market Share Value for Rideshare Service, Insurance Company Contract Length, Insurance Company Annual Cost
External Entity – Insurance Companies (Confidential Data Elements)	IF {((Subject == External Entity) AND (Service Type == Insurance) AND (Service ID == Insurance Identification Number) AND (Session ID = Specific Session Number) AND (Token == Single-Factor One-Time Password (OTP)) AND (Resource == Confidential Data Element) AND (Action == Access))	Longhorn Ride Total Investment Contributions, Longhorn Ride Total Asset Valuation

External Entity – Insurance Companies (Regulatory Data Elements)	IF {((Subject == External Entity) AND (Service Type == Insurance) AND (Service ID == Insurance Identification Number) AND (Session ID = Specific Session Number) AND (Token == Multi-Factor One-Time Password (OTP)) AND (Resource == Regulatory Data Element) AND (Action == Access))	Longhorn Ride Company Liability Insurance, Longhorn Ride Company Number of Office Locations, Longhorn Ride Insurance Policy Identification Number

8 Incident Response Plan

8.1 Incident Identification

In this section, we construct an incident response plan for Longhorn Ride. This ensures that we are able to respond swiftly, efficiently, and appropriately to any occurrence that targets the security of our system – whether it is a security event, security incident, or data breach. This allows us to strengthen the security of our system, address any vulnerabilities within the infrastructure of our system, and provide the highest level of protection to our stakeholders. There are three types of security occurrences: security events, security incidents, and data breaches. A security event is any observable occurrence that occurs in a system or network. A security incident is a specific type of event that violates an organization's privacy and security policies regarding private information. A data breach is a specific type of security incident that results in the disclosure of private information due to unauthorized access to restricted data elements. Possible instances of each of these are defined below; we have also described possible losses (in data, finance, time, and reputation) as well as potential impacts to business continuity as a result of these instances.

Table 9. **Possible Security Events**

Name of Event	Description of Event	Possible Loss (Data, Finances, Time, Reputation)	Concern for Business Continuity (What Portion of Business Operations are Impacted)
System Firewall Blocks Attempted Device Connection	An unknown and unauthorized device tries connecting to our private network. The system firewall blocks the attempted connection made by the unauthorized device. Although the device was not granted access to our private network, it was an occurrence that interacted with our internal systems; thus, it is classified as a security event.	Since the unauthorized device was blocked by our system firewall and unable to connect, there is not a significant amount of loss to data, finances, time, and reputation. In this case, no data was lost since the device was not granted access to our internal system. There was no loss of money, for we did not spend to recover or protect data. We potentially lost a small amount of	In this circumstance, only the technology operations of the business are impacted. Since the device was not granted authorization, no internal information was accessed. The only impact is that the internal system potentially spent a little bit of time and took a slightly increased network load to block the attempted connection.

		time because the system had to block the attempted connection before resuming its scheduled work. The reputation of our company is the same because we successfully prevented an unauthorized device from connecting.	
Suspicious Email Sent to Employee	A suspicious email is sent to one of our internal employees from an unknown source. The employee ignores the email and flags it as malicious within the internal system – which appropriately removes it. Although the employee did not interact with the email, it was an occurrence that interacted with our internal systems; thus, it is classified as a security event.	Since the suspicious email was appropriately flagged and removed, there is not a significant amount of loss to data, finances, time, and reputation. In this case, no data was lost since the employee did not interact with the email. There was no loss of money, for we did not spend to recover or protect data. We potentially lost a small amount of time because the employee had to flag the email. The reputation of our company is the same because we did not interact with the email – thus, no information was lost.	In this circumstance, the employee and the internal system were impacted. Since the employee did not interact with the email, no internal information was accessed. The only impact is that the internal system potentially spent a more time removing the suspicious email and the internal employee spent time to appropriately flag the suspicious email.
Unauthorized Software Download on Company Device	An employee downloads software on a company device without permission. This software is from	There could be a possible loss of data if the downloaded software has access to private device files and	In this case, the technical business operations are impacted because they must spend time

	an unverified source and could be granted access to files on the device. This software download is an occurrence that interacted with our internal systems and devices; thus, it is classified as a security event.	information. There could be a loss of finances if we are required to buy a new device and recover compromised data. There will be a loss of time, for we will spend time removing the software and checking for compromised data elements. Finally, there will be a variable amount of loss to our reputation depending on the intent of the software and its access to private information.	uninstalling software and recovering potentially compromised information. The financial business operations are impacted because a new device might be needed and money could potentially be spent recovering the information. Finally, there could be legal consequences depending on the severity of the circumstance.
Temporary Server/System Outage	The internal system or network crashes and is temporarily unavailable. Nothing is able to interact with the system during this time. This temporary outage is an occurrence that interacted with our internal systems and devices; thus, it is classified as a security event.	The system crash could result in a loss of data within the database. Additionally, there could be a loss of finances to recover corrupted data or invest in additional hardware to prevent future outages. There is a loss of time because internal employees must spend time rebooting the system and users will not be able to access the rideshare platform during that time. There could be a loss of reputation depending on how long the outage lasts, for users will get upset that they	In this circumstance, the technical business operations are impacted because they must spend time rebooting the system and recovering corrupted data. The financial business operations are impacted because no money will be earned from the rideshare platform during the outage. Also, they might have to spend money to buy additional hardware or invest in the infrastructure of the system.

		cannot access the platform.	
Unauthorized Device on Network	An unauthorized device connects to our private network. This device could potentially be malicious; it could also have access to private data elements. This unauthorized access is an occurrence that interacted with our internal systems and devices; thus, it is classified as a security event.	The unauthorized access could result in a loss of data of the device modifies private information. It could also result in a loss of finances if it steals private information because we would have to spend money to recover it. There is a los of time because we need to spend time removing the device from our network. Finally, there could be a loss of reputation depending on whether information was stolen by the unknown device.	In this case, the technology business operations are impacted, for they are required to spend time removing the device from the network and checking if data was compromised. The financial operations could be impacted if we are required to spend money to recover lost information. Finally, the legal operations could be impacted if the device steals sensitive data elements.

Table 10. **Possible Security Incidents**

Name of Incident	Description of Incident	Possible Loss (Data, Finances, Time, Reputation)	Concern for Business Continuity (What Portion of Business Operations are Impacted)
Interaction with a Malicious Email	An employee responds to and interacts with a malicious email from an unidentified source. They click on a link that grants the sender access to private information in the employee's company device. The sender of the malicious email	There is a loss of data because the malicious email accesses and steals private information from the employee's company device. There is a loss of finances, for the company is required to spend money to recover the	In this case, the technology business operations are impacted because they must secure the system and check what data was compromised. The financial business operations are impacted because they must pay for data

	then steals private information from the internal system. Since this resulted in the violation of confidentiality and company policies regarding information privacy and security, it is classified as a security incident. Such an event will have adverse consequences.	information and compensate users. There is a loss of time because employees must spend time seeing which information was compromised. Finally, there is a loss of reputation because the company lost private information.	recovery. Finally, the legal business operations are impacted because they have to check if any regulations were broken by the security incident; they must also notify all affected parties.
Theft of Company Equipment	A burglar steals company device with specific authorization privileges and sensitive information. The thief is then able to access this private information after bypassing the security system of the device. Since this resulted in the violation of confidentiality and company policies regarding information privacy and security, it is classified as a security incident. Such an event will have adverse consequences.	There is a loss of data because the burglar steals and has access to private information on the stolen company device. There is a loss of finances, for the company is required to spend money to recover the information and replace the equipment. There is a loss of time because employees must spend time seeing which information was compromised. Finally, there is a loss of reputation because the company lost private information.	In this circumstance, the technology business operations are impacted because they must secure the system and check what data was compromised. The financial business operations are impacted because they must pay for data recovery and replace the stolen equipment. Finally, the legal business operations are impacted because they have to check if any regulations were broken by the security incident; they must also notify all affected parties.
Unauthorized Device Gains Access to Private Accounts	An unauthorized device joins the network and is given access to private information within the internal system. The device is	There is a loss of data because the unauthorized device has access to private accounts within the internal system. There	In this case, the technology business operations are impacted because they must secure the system and check what data

	also given authorization privileges for access and modification on the system, which allows it to manipulate private data elements. Since this resulted in the violation of confidentiality and company policies regarding information privacy and security, it is classified as a security incident. Such an event will have adverse consequences.	is a loss of finances, for the company is required to spend money to recover the information and strengthen the internal system. There is a loss of time because employees must spend time seeing which information was compromised and must reconfigure a new security system. Finally, there is a loss of reputation because the company lost private information.	was compromised. The financial business operations are impacted because they must pay for data recovery and invest in the security infrastructure of the system. Finally, the legal business operations are impacted because they have to check if any regulations were broken by the security incident; they must also notify all affected parties.
Loss of Physical Files Containing Sensitive Information	An employee loses physical files that contain proprietary company information. Additionally, the files also contain passwords to access the network and internal system. This could lead to a loss of private information if the file lands up in the wrong hands. Since this resulted in the violation of confidentiality and company policies regarding information privacy and security, it is classified as a security incident. Such an event will have adverse consequences.	There is a potential loss of data if a malicious party obtains the lost physical files. There is a loss of finances, for the company is required to spend money to recover the information and replace lost files. There is a loss of time because employees must spend time searching for the file and securing compromised information. Finally, there is a potential loss of reputation depending on where the files end up.	In this case, the technology business operations are impacted because they must check what data was compromised and see if there are digital replacements for the file. The financial business operations are impacted because they must pay to replace the file and potentially pay compensation to affected users. Finally, the legal business operations are impacted because they have to check if any regulations were broken by the security incident; they must

			also notify all affected parties.
Malicious Attack on System Infrastructure	A brute force attack targets our internal systems. It is able to bypass the security measures and is granted authorization privileges. It then uses these privileges to access and steal private information. Since this resulted in the violation of confidentiality and company policies regarding information privacy and security, it is classified as a security incident. Such an event will have adverse consequences.	There is a loss of data because the attackers bypassed the security mechanisms and have access to private information within the network. There is a loss of finances, for the company is required to spend money to recover the information and strengthen the network security systems. There is a loss of time because employees must spend time seeing which information was compromised and must reconfigure a new security system. Finally, there is a loss of reputation because the company was hacked.	In this case, the technology business operations are impacted because they must secure the system, check what data was compromised, and remove the attacker's authorization privileges. The financial business operations are impacted because they must pay for data recovery and invest in the security infrastructure of the system. Finally, the legal business operations are impacted because they have to check if any regulations were broken by the security incident; they must also notify all affected parties.

Table 11. **Possible Data Breaches**

Name of Breach	Description of Breach	Possible Loss (Data, Finances, Time, Reputation)	Concern for Business Continuity (What Portion of Business Operations are Impacted)
Network Security System is Removed	An external party is able to gain access to our private network and gain authorization privileges. They then	There is a loss of data because the external party stole private information and made it public. There is a loss	In this case, the technology business operations are impacted because they must secure the

	use their new credentials to manipulate the network security system and remove it entirely. Private network information is now publicly available and is promptly stolen. Since this resulted in the disclosure of private information and confidential data, it is classified as a data breach. It is more severe than a security incident because it violates information privacy laws and has legal associations.	of finances, for the company is required to spend money to recover the information and reconstruct the network security systems. There is a loss of time because employees must spend time tracing the attack, replacing credentials, and restructuring the system. Finally, there is a loss of reputation because the company lost private information.	internal system, redistribute authorization privileges, and recover information. The financial business operations are impacted because they must pay for data recovery and invest in the security infrastructure of the system. Finally, the legal business operations are impacted because they must also follow legal guidelines and notify/report all affected parties since this involves government regulation.
Attackers Make Private Account Information Public	Attackers are able to bypass our security system and gain authorization privileges. They then access and steal private account information and publish it on another unsecure network. This account information is stolen and manipulated. Since this resulted in the disclosure of private information and confidential data, it is classified as a data breach. It is more severe than a security	There is a loss of data because the attackers stole private user information and published it in a public domain. There is a loss of finances, for the company is required to spend money to recover the information and reconstruct the network security systems. There is a loss of time because employees must spend time tracing the attack, replacing credentials, and restructuring the	In this case, the technology business operations are impacted because they must secure the internal system, redistribute authorization privileges, and recover information. The financial business operations are impacted because they must pay for data recovery and compensate affected users. Finally, the legal business operations are impacted because they

	incident because it violates information privacy laws and has legal associations.	system. Finally, there is a loss of reputation because the company lost private information.	must also follow legal guidelines and notify/report all affected parties since this involves government regulation.
Malicious Program Steals Proprietary Information and IP	Hackers create a malicious program that steals proprietary information from Longhorn Ride. They then use this confidential information to aid direct rideshare competitors. Since this resulted in the disclosure of private information and confidential data, it is classified as a data breach. It is more severe than a security incident because it violates information privacy laws and has legal associations.	There is a loss of company data because hackers created a malicious program to steal intellectual property and proprietary data. There is a loss of finances, for the company is required to spend money to recover the information and reconstruct the network security systems. They also lose market share to their competitors – which is a huge financial loss. There is a loss of time because employees must spend time tracing the attack, replacing credentials, and restructuring the system. Finally, there is a loss of reputation because the company lost private information.	In this case, the technology business operations are impacted because they must secure the internal system and recover information. The financial business operations are impacted because they must pay for data recovery and invest in the security infrastructure of the system. They are also impacted because the intellectual property of the company has been made public, which reduces market share and devalues the company. Finally, the legal business operations are impacted because they must also follow legal guidelines and notify/report all affected parties since this involves government regulation.
Database is Corrupted or Made Public	Attackers infiltrate our network through the database endpoint. They bypass our	There is a loss of data because the database (with all of the data elements from the data	In this case, the technology business operations are impacted because they

	system entirely by targeting the database. They then corrupt the information/make the information public after stealing it. Since this resulted in the disclosure of private information and confidential data, it is classified as a data breach. It is more severe than a security incident because it violates information privacy laws and has legal associations.	inventory) has been corrupted or made public. There is a loss of finances, for the company is required to spend money to recover the information and reconstruct the database endpoints. There is a loss of time because employees must spend time tracing the attack, restructuring the database, and restructuring the system endpoints. Finally, there is a loss of reputation because the company lost private information.	must secure the internal system, reconfigure the database, recreate system endpoints, and recover information. The financial business operations are impacted because they must pay for data recovery and compensate users for lost information. Finally, the legal business operations are impacted because they must also follow legal guidelines and notify/report all affected parties since this involves government regulation.
Users' Financial Information is Stolen	Attackers are able to falsely login as existing users. They then are able to access users' financial information. They proceed to steal this data and lock the account. Since this resulted in the disclosure of private information and confidential data, it is classified as a data breach. It is more severe than a security incident because it violates information privacy laws and has legal associations.	There is a loss of data because attackers were able to impersonate users and steal financial information directly from their account. There is a loss of finances, for the company is required to spend money to recover the information and reconstruct the security systems. There is a loss of time because employees must spend time tracing the attack, replacing credentials,	In this case, the technology business operations are impacted because they must secure the internal system, redistribute authorization privileges, and recover information. The financial business operations are impacted because they must pay for data recovery and invest in the security infrastructure of the system. The financial operations might also

		and restructuring the system. Finally, there is a loss of reputation because the company lost private information.	have to reimburse false charges on the rideshare platform after this data breach. Finally, the legal business operations are impacted because they must also follow legal guidelines and notify/report all affected parties since this involves government regulation.

8.2 Incident Prioritization

Functional Impact Classifications: None, Low, Medium, High
Information Impact Classifications: None, Privacy Breach, Proprietary Breach, Integrity Loss
Recoverability Classifications: Regular, Supplemented, Extended, Not Recoverable

Table 12. **Incident Priority Levels and Associated Criteria**

Incident Priority Level	Criteria (Combination of Functional Impact, Information Impact, and Recoverability)	Why? Justification for the Criteria Specification	Example of Occurrence at Each Level
Level 1	(Functional Impact = None) AND (Information Impact = None) AND (Recoverability = Regular)	A level 1 classification is the lowest incident priority level. It involves public data elements in the information inventory. There is a no functional impact in this type of incident; since the data is already public and there is no loss of private data, there is no impact to our company's ability to continue providing services to users and stakeholders. Additionally, there is no information impact to our organization. No data elements were compromised, accessed, or modified. Thus, the confidentiality, integrity, and availability of information in our data inventory is maintained. The recoverability of information for this type of incident is classified as regular. Since a minimal amount of information is compromised, a minimal amount of time, effort, and money is required to recover information. Additionally, only existing resources are necessary for recovery. A level 1 incident does not impact Longhorn Ride is any significant way.	• The firewall within our internal system blocks an unknown device from connecting and accessing our private network. • An internal employee receives a suspicious email from an unknown source. The employee does not interact with the email and appropriately flags it.
Level 2	(Functional Impact = None OR Functional Impact = Low) AND	A level 2 classification deals with small incidents and minimal impacts to the organization. It	• An employee forgets a USB flash

	(Information Impact = None OR Information Impact = Privacy Breach) AND (Recoverability = Regular OR Recoverability = Supplemented)	involves either low-valued private or public data elements in the information inventory. There is either a low functional impact or no functional impact at all in this type of incident. There is no loss of data when public information is compromised. When proprietary data is compromised, the company loses information that gives it a competitive advantage over other rideshare platforms. We, however, are still able to provide services to all of the stakeholders and users (despite the loss of a competitive advantage). The efficiency and load of our systems might be slightly affected. Furthermore, there is either no information impact or a small breach of private information in this level. Some private data elements and PII are accessed; this access results in a reduced competitive advantage when these types of data elements are lost. Very few data elements were compromised, accessed, or modified in this type of incident. Thus, the confidentiality, integrity, and availability of information in our data inventory is generally maintained. The recoverability of information for this type of incident is classified as regular or supplemented. Since only some data elements amount of are compromised, a minimal amount of time, effort, and money is required to recover information. Additionally, this recovery can be accomplished with existing resources and some additional resources. A	drive with private company information at home. This is a security incident that could result in the loss of proprietary information that could impact the company and reduce their competitive advantage over other rideshare platforms. • An unauthorized device gains credentials to access private company files with information regarding market share and revenue. This information is leaked to rideshare competitors.

		level 2 incident has a minimal impact on Longhorn Ride.	
Level 3	(Functional Impact = Low OR Functional Impact = Medium) AND (Information Impact = Privacy Breach OR Information Impact = Proprietary Breach) AND (Recoverability = Supplemented OR Recoverability = Extended)	A level 3 classification includes significant impacts to the organization; although the organization may still be able to provide essential services, there is a sizeable amount of information that is affected. This incident level involves confidential and proprietary data elements in the information inventory. The functional impact of this type of incident ranges from low to medium; private information of all associated stakeholders is compromised. Due to this, the organization is unable to provide certain services and its business functionalities are impacted. Additionally, there is significant information impact to our company. A level 3 incident includes a privacy breach or a proprietary breach. Many higher-valued data elements within the information inventory are compromised, accessed, and modified. Thus, the confidentiality, integrity, and availability of information in our data inventory is violated for many elements. In addition, the company loses its proprietary data (resulting in a reduced competitive advantage) and the stakeholders (as well as their associated confidential data) is impacted. The recoverability of information for this type of incident is classified as supplemented or extended. Since a sizeable amount of information is compromised, a significant amount of time, effort, and money is required to recover information.	• An internal employee interacts with a malicious mail from an unknown source. An attacker is then able to take control of the company device and access confidential and proprietary data. This impacts the business functionalities of Longhorn Ride and compromises stakeholder information. It also reduces Longhorn Ride's market share and competitive advantage. • An unauthorized device gains access to our private network and is able to see confidential stakeholder information and PII.

		Furthermore, the recovery process requires resources; the amount of time such a recovery could take might also be unpredictable. A level 3 incident significantly impacts Longhorn Ride and its stakeholders.	
Level 4	(Functional Impact = Medium OR Functional Impact = High) AND (Information Impact = Proprietary Breach OR Information Impact = Integrity Loss) AND (Recoverability = Extended OR Recoverability = Not Recoverable)	A level 4 classification entails significant impacts to the organization and large security incidents. It involves confidential and regulatory data within the organization's information inventory. There is a medium to high functional impact on the company's business continuity. Due to the loss of private information, the company is unable to provide many of its services and many stakeholders on the rideshare platform are impacted. The business continuity of Longhorn Ride (current and future) is impacted in such a way that the business must change in order to continue operating. Furthermore, there is a significant information impact consisting of a proprietary breach and a loss of integrity. Many private data elements within the information inventory are compromised, accessed and modified. The scope of compromised data elements impacts the company (in terms of competitive advantages and market share) as well as users (in terms of compromised PII). Thus, the confidentiality, integrity, and availability of information in our data inventory is violated. The recoverability of information for this type of incident is classified as extended. In some cases, the information might not even be	• Hackers disable part of the security system within our private network. They are then able to access and modify private information such as proprietary business information and confidential stakeholder PII. They are also able to access low-valued regulatory data. This impacts the operations of Longhorn Rides and devalues our reputation. • Hackers are able to falsely login to users' private accounts and order rides. This compromises their PII and impacts the rideshare services that Longhorn Ride provides. We must reimburse users for false rides and secure our internal system.

		recoverable. Since many data elements are compromised, a significant amount of time, effort, and money is required to recover information. Additionally, many additional resources are necessary to recover the large amount of compromised data. In some extreme cases, the information might not be recoverable at all. This type of incident is characterized by a very unpredictable recovery process that will impact the business heavily. A level 4 incident will have a significant impact on Longhorn Ride and impact all of its associated stakeholders in a significant manner.	
Level 5	(Functional Impact = High) AND (Information Impact = Integrity Loss) AND (Recoverability = Not Recoverable)	A level 5 classification refers to a huge security incident that severely impacts Longhorn Ride and its stakeholders. Such a high-priority incident will require a tremendous amount of resources and will change the company indefinitely. This incident level involves regulatory data elements in the information inventory – which are the most restricted data elements within our system. The functional impact of this type of incident is extremely high; all private information related to all associated stakeholders is compromised. Due to this, the organization is unable to provide any services or rideshare functionalities to any users. Additionally, there is gargantuan information impact to our company. A level 5 incident means that there is a loss of integrity for all data elements within our information inventory. All data elements	• A team of hackers is able to infiltrate our private network and remove the security mechanisms of our internal system. They then proceed to steal regulatory information such as users' credit card information. They also take the social security numbers of all internal employees. Finally, they corrupt all of the data and leave the internal system in a broken state. This significantly impacts the business operations of Longhorn Ride. Additionally, it also

		within the information inventory are compromised, accessed, and modified. Thus, the confidentiality, integrity, and availability of information in our entire data inventory is violated. In addition, the company is unable to protect regulatory data elements, which reduces the value of the company, exposes competitive advantages, and compromises all stakeholders (users, investors, and internal employees). There is no possibility of recovering al information from an incident of this caliber. Since most of the information within the data inventory is compromised, a significant amount of time, effort, and money is required to recover information. Furthermore, the recovery of information, if possible, will be unpredictable and will require additional resources along with external intervention. A level 5 incident significantly impacts Longhorn Ride and its stakeholders. In fact, the company might not be able to survive after such an incident. If it does, it will be changed indefinitely and must undergo heavy restructuring.	impacts all of their stakeholders and users. The technology team must repair the system and recover the information (if possible). The financial teams must compensate stakeholders and pay for damages. The legal team must comply with governmental regulations and notify all affected parties. • The database where all of the data elements from the information inventory are stored is attacked. The database is made public and all of the data elements are stolen. This severely impacts the operation of the business. All rideshare services must be stopped until the system is secured and information is traced appropriately. Longhorn Ride must also contact all impacted parties.

8.3 Incident Response Team

Table 13. **Incident Response Team – Roles and Responsibilities**

Incident Response Team Member Role	Incident Response Team Member Responsibility
Incident Lead (Executive Board Member of Longhorn Ride)	The incident lead is defined as the head of the internal incident response team. They are tasked with maintaining the incident response plan, organizing efforts within the team, coordinating recurring sessions regarding investing in the security infrastructure of the internal system, and mobilizing different units when a security incident occurs. The incident lead is typically from an outside counsel – a group that is not directly involved with the configuration of internal security systems. In this case, the incident lead is an executive board member of Longhorn Ride. During an incident, they must ensure that all members of the incident response team are appropriately following the established guidelines; they must also appropriately address issues that were not enumerated in the response plan by reaching out to the correct incident response team members.
Technician/Security Engineer (Internal Employee – IT Department)	A technician/security engineer is the technical specialist that directly configures the internal security system and is able to manipulate information within the data inventory. There will be a team of multiple technicians and security engineers dedicated to the incident response team. Apart from their usual role of designing digital systems that protect against cyber attacks and constructing security mechanisms that prevent unauthorized access to the internal system, they will also respond directly to security incidents as they occur by immediately patching the system. There will always be a few members of this team that are always on-call; they will have rotational shifts so that they can always address a security concern. If the system is bypassed or attacked, they will patch the system and immediately secure information until an appropriate fix or redesign of the internal system is constructed. They also have the ability to shutdown the network in order to stop all network activity.
Public Relations Expert (Internal Employee – HR Department)	The public relations expert is an internal employee that is part of the HR department. They are in charge of drafting communications plans and appropriately contacting stakeholders for different security incident levels. They focus on notifying

	individuals that are not on any internal teams within Longhorn Ride. They focus on contacting and notifying stakeholders (such as riders, drivers, investors, third-party cloud storage vendors, and external entities) as well as the general public. Their main goal is to effectively communicate information about security incidents to the affected parties. They must also ensure that the reputation and value of the organization is maintained by effectively communicating security indents and portraying the organization in a positive manner.
Human Resources Employee **(**Internal Employee – HR Department**)**	The human resources employee focuses on notifying individuals that are employees within the organization and individuals that have internal roles. Similar to the public relations expert, they are in charge of drafting communications plans and contacting employees for different security incident levels. Their communication focuses more on contacting individuals within Longhorn Ride (such as internal employees within the IT and HR departments as well as the executive company board of Longhorn Ride). They must ensure that everyone within Longhorn Ride knows what the next steps following a security incident are; additionally, they must ensure that internal employees are appropriately updated and notified.
Customer Support Employee **(**Internal Employee – IT Department**)**	The customer support employee focuses on addressing questions, concerns, and issues brought up by users on our rideshare platform. They must address and help fix specific issues brought up by riders and drivers that use our application. They must also communicate these user concerns to the development and securities team so that they can address these issues in a system-wide context. We will have a customer support team that is on-call; they will have rotational shifts so that someone is always monitoring the situation. The primary aim of this role is to address user issues and also communicate potential security incidents to the rest of the incident response team.
Legal Advisor	The legal advisor focuses on ensuring that our organization complies with laws and regulations regarding data breaches. They check to see if a security incident falls under government regulations (such as the GDPR) and they make sure that the organization takes the necessary legal steps during a security incident. They are also tasked with communicating information regarding security

	incidents to the public; they work in accordance with the public relations expert in order to make sure that stakeholders, users, and the public are informed of any data breaches. They also help minimize liabilities associated with information and help with potential lawsuits during a data breach.
Law Enforcement	Law enforcement is only brought in during severe data breaches and security incidents. They operate independently from the organization that requests their help. They open investigations to see who stole the data, how it was stolen, why it was stolen, and what potential risks could impact the public following the security incident. They operate under government regulations and require that private company information be made public. They also work in accordance with the company to address the public, trace lost information, and resolve the security incident.

8.4 Incident Response Playbook – Notification Plan

Table 14. **Incident Response Notification Plan**

Incident	Notify Which Roles	Notification Method	Notification Timing (Specified in Terms of Upper Limit Time After Discovery)
Level 1	• Incident Lead • Technician/Security Engineer	• Secure email or internal company message to incident response team (incident lead and technician/security engineer)	Within 6 Hours of Discovery
Level 2	• Incident Lead • Technician/Security Engineer • Human Resources Employee • Customer Support Employee • Legal Advisor • Executive Company Board of Longhorn Ride	• Secure email or internal company message to incident response team (incident lead, technician/security engineer, human resources employee, customer support employee, legal advisor) • Secure email or internal company message to executive company board • Immediate phone call to incident response team (incident lead, technician/security engineer, human resources employee, customer support employee, legal advisor)	Within 3 Hours of Discovery
Level 3	• Incident Lead • Technician/Security Engineer • Public Relations Expert • Human Resources Employee • Customer Support Employee • Legal Advisor • Executive Company Board of Longhorn Ride	• Secure email or internal company message to incident response team (incident lead, technician/security engineer, public relations expert, human resources employee, customer support employee, legal advisor) • Secure email or internal company message to	Within 1 Hour of Discovery

	• Internal Employees – IT Department • Internal Employees – HR Department • External Entities – Insurance Companies	executive company board • Secure email or internal company message to internal employees (IT and HR departments) • Immediate phone call to incident response team (incident lead, technician/security engineer, public relations expert, human resources employee, customer support employee, legal advisor) • Immediate phone call to executive company board • Formal email to external entities – insurance companies • Formal letter to external entities – insurance companies • Formal claim to external entities – insurance companies	
Level 4	• Incident Lead • Technician/Security Engineer • Public Relations Expert • Human Resources Employee • Customer Support Employee • Legal Advisor • Executive Company Board of Longhorn Ride • Internal Employees – IT Department • Internal Employees – HR Department • Riders • Drivers • Investors • External Entities – Insurance Companies	• Secure email or internal company message to incident response team (incident lead, technician/security engineer, public relations expert, human resources employee, customer support employee, legal advisor) • Secure email or internal company message to executive company board • Secure email or internal company message to internal employees (IT and HR departments) • Immediate phone call to incident response team	Within 30 Minutes of Discovery

	- Third-Party Cloud Storage Vendor	(incident lead, technician/security engineer, public relations expert, human resources employee, customer support employee, legal advisor) - Immediate phone call to executive company board - Formal email to stakeholders (riders, drivers, investors) - Formal letter to stakeholders (riders, drivers, investors) - Formal email to external entities – insurance companies - Formal letter to external entities – insurance companies - Formal claim to external entities – insurance companies - Formal email to third-party cloud storage vendor - Formal letter to third-party cloud storage vendor	
Level 5	- Incident Lead - Technician/Security Engineer - Public Relations Expert - Human Resources Employee - Customer Support Employee - Legal Advisor - Executive Company Board of Longhorn Ride - Internal Employees – IT Department - Internal Employees – HR Department - Riders	- Secure email or internal company message to incident response team (incident lead, technician/security engineer, public relations expert, human resources employee, customer support employee, legal advisor) - Secure email or internal company message to executive company board - Secure email or internal company message to	Within 15 Minutes of Discovery

	• Drivers • Investors • External Entities – Insurance Companies • Third-Party Cloud Storage Vendor • The Government • Law Enforcement • The Public	internal employees (IT and HR departments) • Immediate phone call to incident response team (incident lead, technician/security engineer, public relations expert, human resources employee, customer support employee, legal advisor) • Immediate phone call to executive company board • Formal email to stakeholders (riders, drivers, investors) • Formal letter to stakeholders (riders, drivers, investors) • Formal email to external entities – insurance companies • Formal letter to external entities – insurance companies • Formal claim to external entities – insurance companies • Formal email to third-party cloud storage vendor • Formal letter to third-party cloud storage vendor • Formal email to the government • Formal letter to the government • Formal legal documents for the government • Formal email to law enforcement • Formal letter to law enforcement • Formal request for law enforcement	

		• Formal email to the public • Formal letter to the public	

9 Information Security and Privacy: Trust Frameworks, Technology and Design Principles

9.1 Trust Framework

Longhorn Ride uses the **Centralized Single Sign-On** trust framework. It is the most optimal type of trust framework for our purpose, and it provides the highest level of information security for our stakeholders and data owners. Centralized Single Sign-On is a framework that allows users to access multiple applications with only one type of credential. The authentication process is structured so that a user only needs a single set of credentials that gives them access to data and organizations within the trust framework.

The Centralized Single Sign-On trust framework has many benefits. To begin, this framework is associated with the highest level of user convenience, for users are only required to sign-in once. They are not required to keep track of multiple tokens; they only require one set of credentials to login. Once signed-in, users are given permission to access multiple entities and service providers. Additionally, this framework is associated with the one of the best authentication implementations, for there is a single, centralized control point. Since a group of relying parties are required to agree upon a centralized and standardized set of protocols for this framework, the authentication strength of the application is maximized. Thus, the authentication strength for this framework is one of the best. However, one tradeoff of this system is that it is difficult to construct; organizations must collaborate as well as invest a time, money, and effort to make congruent across all involved parties and applications. This means that this framework has a low service provider ease-of-implementation. Finally, this framework is able to scale effectively as the number of users increases. This framework is able to add organizations and applications that satisfy the established requirements; thus, scaling this framework is easy and effective.

9.2 Select Technology Solutions for Selected Trust Framework

Table 15. **Technology Solutions for Centralized Single Sign-On Trust Framework**

	Data Classification	Technology and Design Principles	CIA Protection	Rationale for Selected Technologies and Methods
Data at Rest	Public, Proprietary, Confidential, Regulatory	Technology: Encryption (Symmetric and Asymmetric) Design Principle: Least Common Mechanism	Encryption: • Confidentiality Least Common Mechanism: • Confidentiality • Integrity • Availability	Encryption: Encryption ensures that only authorized parties are able to access and view sensitive data. It is important to encrypt data at rest so that even if unauthorized parties are able to reach the data, they are unable to comprehend it. One example is encrypting data in a shared cloud database. If other cloud customers somehow gain access to our private information, they are unable to view it. This mitigates confidentiality and shared resource threats. Least Common Mechanism: This design principle states that security mechanisms that allow users to access resources and private data should not be shared. This ensures confidentiality, for only authorized parties are able to view sensitive data. This ensures integrity because only authorized parties are able to modify private information. Finally, it ensures availability because the information is always in an appropriate state and is always accessible to authorized users.

Data in Transit	Public, Proprietary, Confidential, Regulatory	Technology: Digital Signatures Design Principle: Least Privilege	Digital Signatures: • Confidentiality • Integrity Least Privilege: • Confidentiality • Integrity • Availability	Digital Signatures: Digital signatures maintain the confidentiality and integrity of information. Digital signatures employ encryption; thus, they are only accessible to authorized parties and users. Digital signatures also use message digests; this allows recipients to know whether or not the data has been modified – which preserves integrity. Digital signatures also maintain authenticity. It ensures that data in transit from one party to another is always protected. Least Privilege: This design principle states that a program or user should only be given the minimum credentials or privileges required to accomplish certain functions. This maintains confidentiality because only authorized parties are allowed to access data for certain jobs. This also maintains integrity because parties can only modify information that they are authorized to interact with. Finally, it maintains availability, for private data is always available at the appropriate time and form for authorized individuals. Only the authorized parties are able to access and modify the data during transit. Thus, the data is always available.

Access to Data	Public, Proprietary, Confidential, Regulatory	Technology: Firewalls Design Principle: Fail-Safe Defaults	Firewalls: • Confidentiality • Availability Fail-Safe Defaults: • Confidentiality • Integrity • Availability	Firewalls: Firewalls ensure the confidentiality and availability of information. They filter transmitted information between a known, private network and an external network. Data on the private network can only be accessed by authorized individuals; thus, confidentiality is maintained. Data is also in the appropriate state and always available to those with the appropriate credentials, thus, the availability of private information is maintained. Fail-Safe Defaults: This design principle states that all parties are denied access and modification privileges by default. In order to obtain the appropriate credentials, parties must be explicitly given privileges for a specific resource. This ensures the confidentiality of data because only authorized individuals are able to access private information. It also ensures the integrity of the data because only authorized individuals are able to modify the data. Finally, it ensures the availability of information because data will always be available and in the appropriate state to those with access and modification privileges; it is unavailable to everybody else.

9.3 Solution Set for Network and Web Security

Table 16. **Network and Web Security Solutions**

	Solution	Solution Description	Mitigated Risks and Threats	Improvements to Confidentiality, Integrity, Availability, and Authenticity
1	**Encryption (Symmetric and Asymmetric)**	Encryption is the process of encoding data so that is not viewable or accessible by unauthorized parties. Only individuals that have the appropriate key to decrypt the information are able to access encrypted data. Thus, confidentiality of the information is maintained. For symmetric encryption, one key is used to both encrypt and decrypt information. Confidentiality is preserved because only authorized parties that have the private key are able to see encrypted data. For asymmetric encryption, there is a public key and a private key. The public key is used to encrypt information and only the party with the private key is able to view such information. This protects information against confidentiality threats.	Symmetric encryption protects access to files, messages, and data. Asymmetric encryption protects the exchange of keys and access to keys. Together, they can be used in procedure called Pretty Good Privacy (PGP), which is used to exchange keys, maintain confidentiality, and create secure channels. They mitigate risks associated with loss of private data to unauthorized parties.	• Confidentiality
2	**Digital Signatures**	Digital signatures ensure the authenticity, non-repudiation, integrity, and new nature of information. They encrypt the message digest and the contents of the file so that only the authorized parties	Digital signatures protect access to the content of sensitive files, keys, and private information. Digital signatures also illustrate the	• Confidentiality • Integrity • Authenticity

		with the appropriate keys are able to access the data. This protects against confidentiality threats, for information access is granted to authorized parties with the appropriate keys and denied to everyone else. Additionally, digital signatures maintain integrity by using a secure hash code to calculate a message digest that is included as part of the digital signature. The message digest is also encrypted for added security. If the message digest matches the expected value, the recipient can be sure that the contents of the file have not been modified. Thus, digital signatures protect against integrity threats.	authenticity of data and guarantee that such information comes from the signer. They mitigate threats associated with man-in-the-middle attacks.	
3	**Firewalls**	Firewalls manage data transmission between two networks – usually an external network and an internal (private) network. Firewalls filter out any data that does not satisfy predetermined rules and firewall protocols. They also restrict access to private information and internal servers to unauthorized parties. Firewalls protect against confidentiality threats by ensuring that only authorized parties with the appropriate credentials are allowed to access and view private information. All other parties	Firewalls protect the availability of information on servers and networks. They mitigate the risks and threats associated with intrusions on private networks.	• Confidentiality • Availability • Authenticity

		do not gain access to such private data. Additionally, firewalls guarantee that information is always available in the appropriate state for authorized users. They prevent any unauthorized parties from accessing and modifying information; only verified individuals with the appropriate credentials are able to interact with sensitive information. Thus, the availability of the data is maintained, for it will be in an appropriate state managed by the network administrators and the firewall.		
4	**Message Digests (Error Codes)**	Message digests (error codes) are used to illustrate the integrity of information. On their own, they are not enough to maintain the confidentiality or authenticity of data. A message digest is calculated from the content of the file. If the transmitted data has a different message digest value than what was calculated, the recipient will know that the contents of the file have been modified. If they are the same, the recipient can be sure that the integrity of that data has been maintained. Thus, message digests protect against integrity threats.	Error codes and message digests protect the integrity of messages and files. They ensure that the content has not been modified. They mitigate risks associated with the unauthorized modification and corruption of private information. They protect messages and the content of files during transmission.	• Integrity
5	**Intrusion Detection Tools**	Intrusion detection tools are able to construct models of appropriate behaviors and	Intrusion detection tools protect the availability of	• Confidentiality • Availability

		conduct pattern-matching in order to restrict access to the network or allow authorized parties to interact with private data. This means that only authorized parties that do not exhibit suspicious behavior are allowed to access and modify with private data. This means that the sensitive information on the network will always be available and in an appropriate state for verified parties. Thus, intrusion detection tools protect against availability threats. Additionally, they maintain the confidentiality of information, for only authorized users are able to access and view private data. Intrusion detection tools will block any party with inadequate credentials; thus, confidentiality is maintained.	information during transactions and the transmission of data. They mitigate the threats and risks associated with unauthorized access during transmission. An example of a threat that it mitigates is the man-in-the-middle attack.	
6	**Virus Detectors**	Virus detectors are programs and applications that are able to discover malicious programs through a pattern recognition process. They look for indications of inappropriate data access or modification in files and systems containing private data. If there is no unauthorized access or modification detected, individuals are able to interact with the information in its intended state at any time. Thus, virus detectors protect	Virus detectors protect the availability of information in code, programs, files, and private repositories that store data. They mitigate risks and threats associated with unauthorized modification and corruption. Examples of threats they combat include malicious software that corrupts	• Integrity • Availability

		against availability threats. In addition, virus detectors ensure the integrity of information. If a private file is modified by an unauthorized party, the virus detector will block changes and revert the contents of the file back to its original state. Thus, the integrity of data is maintained.	databases and intensive programs that could put strain on the network. Unauthorized applications that run on a private network could have an extreme number of requests and place a heavy load on the network; this would reduce the ability of our internal system to maintain the availability of information.	
7	**SSL Certificates and https**	SSL Certificates allow a device to form an encrypted and secure connection with a server on the internet. That is why https includes the “s” character; it means that the channel is secure. SSL certificates ensure that information transmitted between the device and the web server is secure; this is accomplished through encryption. Thus, only authorized parties are able to access and view information. Additionally, the authenticity of data is maintained. Parties are only allowed to obtain SSL certificates if they have been verified by an external organization. Thus, the information transmitted by such a party is authentic and trustworthy.	SSL Certificates and secure channels with https mitigate risks associated with confidentiality and authenticity. They reduce the possibility of man-in-the-middle attacks while using the internet. They also mitigate the threats and risks associated with data loss on the internet. Only authorized parties are able to access, view, and interact with private information.	• Confidentiality • Authenticity