# CIT 285 - Lab #11: Policy and IR plan

**Kaleb Alstott**

**Spatula City**

**100 Nunn Drive**

**Highland Heights, KY 41099**

## Policy

**1.1 Policy Name**

**Data loss prevention policy**

**1.2 Overview and Scope Statement**

Data is one of the most valued resources we hold as a company and we want to do everything we can to make sure our data is safe and protected at all times. Data loss prevention is a set of tools and processes set up and used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

The purpose of this policy is to define the requirements for the data loss prevention policy. A company as a whole has decided to ensure a more safe and easier way to ensure our data is safe and protected at all times. If you are reading this and are a part of our data scientist team, data analysis team, or deal with our data as a company we need you to follow these policy statements.

**1.3 Policy Statement**

Here are the steps we need to take to protect our data

1. Identify and classify important information of sensitive data
   1. Implementing an access control list
2. Data encryption
   1. Both software and hardware base encryption. All critical business data should be encrypted while at rest or in transit. Portable devices should use encrypted disk solutions if they will hold any important data.
3. Hardened systems
4. Strict allocation of roles
   1. Clearly define the role of each individual involved with the data. Specify who owns which data and what they can do with it.
5. Implementing regular management system checks
   1. This will include keeping OS up to date. Checking all security to make sure everything is up to the best and newest form.
6. Don’t save unnecessary data, only when needed should we be saving data

**1.4 Accountability Statement**

Accountability is the requirement that loss data or hacked data will be on you and your team. From a business standpoint of view this data builds, shapes, and grows this company. Not adhering to the steps outlined in this policy will result in but are not limited to; official reprimand, loss of job responsibilities and termination of employment.

**1.5 Exception Statement**

In the event the steps detailed in this policy cannot be followed we as a company will find new employs who will care about the growth and safety of our company. Thank you

**Spatula City**

**100 Nunn Drive**

**Highland Heights, KY 41099**

## Incident Response Plan

*Incident Scenario*

We have came across a weekly report saying we have had a breach in our systems and have found out how the intruder was able to access our data. We seem to have a classic phishing attack on the company and has been a human error clicking on this link or webmail and putting our company at risk. Luckily as of now we have secured our data base but next time we need to be more careful and watch out for these phishing attacks.

*Incident Response Cycle*

**Phase 1: Identifying**

When we are looking at this phishing attack, we know it has to be a human error. When looking into human errors this could take forever to narrow down due to figuring out who clicked on what webmail and when.

**Phase 2: Investigating**

When investigation this attack, we need to understand what type of human error occurred and why. Was this phishing attack easy to be detected or was it hard to notice if it was an attack? Was the attack sent to one person or to every employer? Is there more attacks or past attacks from the same person? When investigation we need to look at every email that has been sent to every individual and see when and who clicked on this webmail to allow access to our company’s data.

**Phase 3: Repairing**

When repairing this attack, we need to first go back and look into a phishing detection software to limit these occurrences. I would use Brandshield anti-phishing software to limit the occurrence and use of a phishing attack. I would then have to go back and start new encryptions on our data to make sure that the information that the attacker was able to get is limited and not accessible anymore. Lastly, we would have a conference going over how to spot phishing emails and how we can stop them. Making sure to keep an eye out for suspicious activity, missed spelled words, important information being asked of you, and much more.

**Phase 4: Documenting**

When documenting we would write down the occurrence, find out who accessed this email and go about a meeting with what was given and if and why did they access this email. We would document the new encryptions and make notes to schedule and set up a download of the new software

**Phase 5: Adjusting Procedures**

When looking at this type of attack, this is a common human error occurrence and when adding to the procedure we would have added the anti-phishing software in hope to limit and stop these attacks. Hopefully after the meetings, system checks, and anti-phishing software we can run a productive growing data analysis company.