# Digital Portfolio Project

1. **Administrative Controls:**

**ADMINISTRATIVE – DETERRENT – POLICY:**

**DESCRIPTION:** A policy is something put in place by management to inform employees of anything they need to know about how to do things the right way. If the policy is not followed by employees, it can usually lead to lawsuits and other problems in the workplace. The policy acts as a deterrent by informing employees of what not to do, while also providing them with a clear idea of what will happen if they do not follow the policy. A good example of a policy would be a policy for customer support representatives on how to act during calls; this might be put in place to help avoid social engineering attacks. This policy would explicitly inform them on how to deal with possible social engineering attacks, as well as explain what will happen if the attack is successful due to failure on the employee’s part (usually termination, but sometimes this can result in lawsuits and jail time).

**ADMINISTRATIVE – PREVENTATIVE – USER REGISTRATION POLICY:**

**DESCRIPTION:** A user registration policy is a policy put into place by management that informs employees how to register for certain user accounts. The accounts that must be registered are almost always web based (since most companies tend to employ the help of other companies by using their software to automate tasks in the workplace) so the policy helps users register safely. When a website tells you to include a special character or use a certain amount of characters in your password, that is *their* user registration policy for *their* services to *you*. These are usually put in place to help secure user accounts and to prevent them from being hijacked by attackers. Instead of a screenshot, I will link the Twitter rules (i.e., their user registration policy for creating an account on their site) <https://help.twitter.com/en/rules-and-policies/twitter-rules>.

**ADMINISTRATIVE – DETECTIVE – REVIEW VIOLATION REPORTS:**

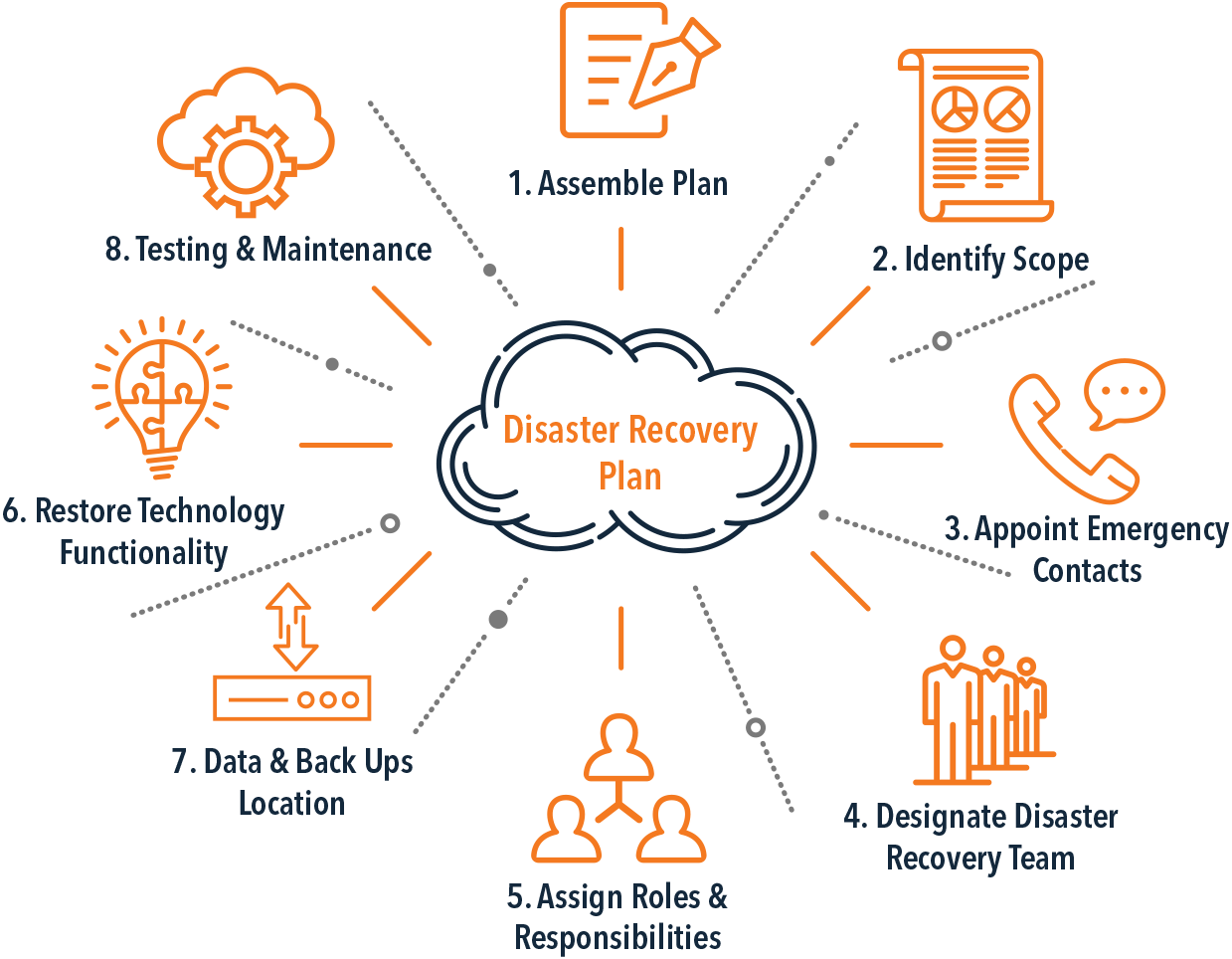
**DESCRIPTION:** If there has been a workplace violation, the business must look through old violation reports to determine if this has been a reoccurring incident. For example, if an employee has been accused of sexual misconduct in the office and past violation reports show that he has been accused before, it will help build a case against the employee to get them fired. It is important to keep violation reports filed neatly in the office to help with timely violation report reviewing, or alternatively stored electronically to help with accessibility. Any employee that wants to submit a tip about a workplace violation should be able to submit that tip anonymously (either electronically or physically).

**ADMINISTRATIVE – CORRECTIVE – TERMINATION:**

**DESCRIPTION:** Termination is the corrective procedure that is employed when a company policy/rule is violated by an employee. By firing the employee, the company is avoiding a lot of liability that might ensue if they were to keep them in their employment. While the action that the employee does may not always seem reasonable to fire them over, it is usually due to them violating a part of a contract they sign when they were hired by the company. A good example of this happening in the real world is the Edward Snowden case; after leaking important classified information from the NSA (and more importantly, violating many contracts and laws) he was terminated from working with the Central Intelligence Agency (CIA).

**ADMINISTRATIVE – RECOVERY – DISASTER RECOVERY PLAN:**

**DESCRIPTION:** A disaster recovery plan is a plan that was created to be used in the event of a workplace disaster. The DR plan tries to prepare for any disaster by being general when describing the vulnerabilities and threats; this way the actions listed could be used for more than one situation. When a disaster strikes, it is assumed the business will be unable to operate and generate income for themselves; it is because of this that the DR plan is one of the most important things in a business. If a disaster were to happen and the company could not fix it or generate any income in the meantime to try to deal with it, it would bankrupt the entire business. I am attaching an image as an example that illustrates the most important things to do within a DR plan.



**ADMINISTRATIVE – COMPENSATING – JOB ROTATION:**

**DESCRIPTION:** Job rotation is the act of rotating specific job responsibilities between employees so that no one employee is directly in control of a job function. If a single employee was the only one that could do a specific function in the workplace, he/she becomes the Single Point of Failure (SPoF) for that business. If jobs are rotated, multiple employees become responsible for single job functions; this compensates for a lot of security problems that may exist within the business. This process also helps employees cross-train other employees and gives them all a wider range of skills to use in the business.

1. **Technical Controls:**

**TECHNICAL – DETERRENT – WARNING BANNERS:**

**DESCRIPTION:** Warning banners are used to deter unauthorized access to company systems. These are mostly used on company tools/machines that can be remote accessed; by putting a banner onto the remote gateway, anybody accessing the tool/machine will be aware of what the banner says. If incoming remote connections are warned that accessing the tool/machine without the proper authority is a federal crime, you effectively deter some unauthorized intruders from connecting. Below I have included a screencap of the login page for Paloalto; the warning banner is meant to deter unauthorized access to existing accounts.



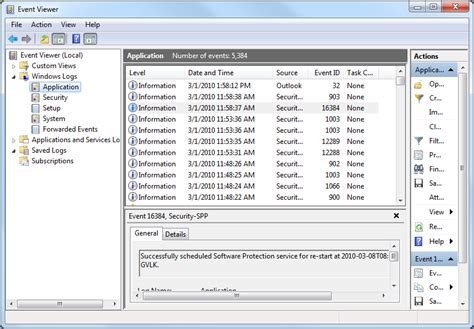
**TECHNICAL – PREVENTATIVE – PASSWORDS:**

**DESCRIPTION:** Passwords are used to help authenticate a user based on what they know to help secure accounts. These are helpful in preventing attacks like social engineering and unauthorized data mining but are still susceptible to attacks. Some attacks that a system entirely dependent on password-based logins may be susceptible to are passwords crackers, keyloggers, shoulder surfing and malicious software. With 2-Factor Authentication (2FA) this can help protect a web-based service and its’ users from being open to outside attacks. The example I’m providing below is a web portal for Comcast employees to login to use employee tools; while it is open to the Internet for anyone to find, you need a password (and form of 2FA, in this case the CABLE or CORPHQ NT ID) in order to access the system, which will help prevent unauthorized access to the employee tools.



**TECHNICAL – DETECTIVE – LOGS:**

**DESCRIPTION:** Logs generally refer to the storage of data on a machine that can help identify what any user at any given time was doing. This is generally to help identify an incident that has occurred in the workplace. Management will usually install a program on the machines that will silently collect information in the background while employees do their usual tasks. If an incident were to occur (breach in a public facing web server, an employee web account has been hijacked, etc.) the logs could be investigated and it could be determined where the source of the problem occurred at; if an employee is responsible for a data breach or large attack, the evidence will be on the logs on their company machine. I have included a screenshot below of the Windows Event Logs, which is a log of general information in relation to any Windows Event.



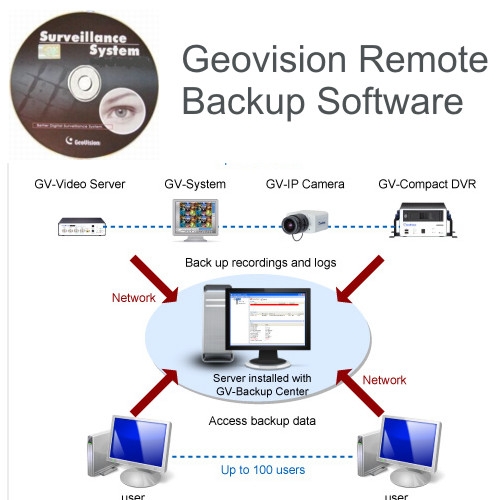
**TECHNICAL – CORRECTIVE – TERMINATE CONNECTION:**

**DESCRIPTION:** If a computer is infected with malware and has a chance of infecting other machines on the network, the corrective action to take would be to terminate the connection; this could be either a connection to the local network or the power connection to the computer. This is a corrective action because it corrects the problem temporarily; if the machine is infected, you don’t want every other machine in the business to be infected, so you have *temporarily* terminated the connection to the network until the machine is fixed. While this is not a permanent fix and does not work in every situation, it helps with a majority of situations to help correct the problem and stop it from progressing into a worse problem. I am providing a picture of the ethernet cable being unplugged from the router to help signify exactly what I am describing.



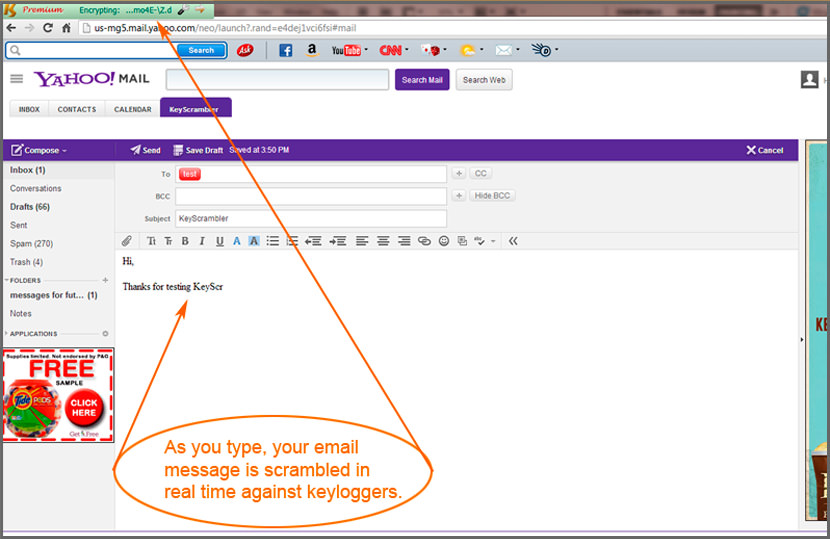
**TECHNICAL – RECOVERY – TAPE BACKUPS:**

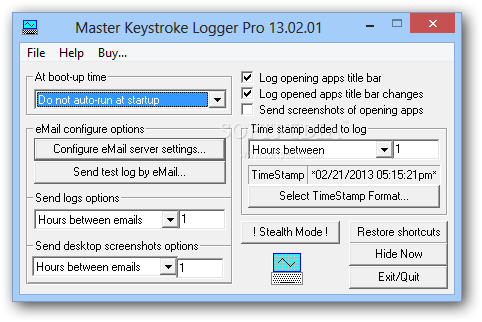
**DESCRIPTION:** Tape backups are any backups of CCTV footage from the business stored either offsite or onsite. These are classified as recovery access controls because the business will have a way to restore conditions to normal in the event of a disaster. For example, if an employee was caught stealing sensitive data on a CCTV camera and then destroyed the local copies of the tapes, the backups are saved somewhere else and can be used to prosecute the employee and restore working conditions back to normal. I am providing an example of how these tape backups are stored and accessed if you were to store the tape backups with Geovision Remote Backup Software.



**TECHNICAL – COMPENSATING – KEYSTROKE MONITORING:**

**DESCRIPTION:** Keystroke monitoring is a way of monitoring what all employees are doing without constantly having to supervise them. Using software that accomplishes this will help management prevent malicious activity and misuse of company resources. There is software that exists that can obfuscate key strokes and make this software effectively useless; programs such as KeyScrambler (<https://www.qfxsoftware.com/>) can encrypt all keystrokes into random characters so that it is impossible to determine what the user is typing. The two pictures I am providing below relate to this; the first is a screenshot of KeyScrambler being used and the second is a screenshot of a keystroke monitoring program.

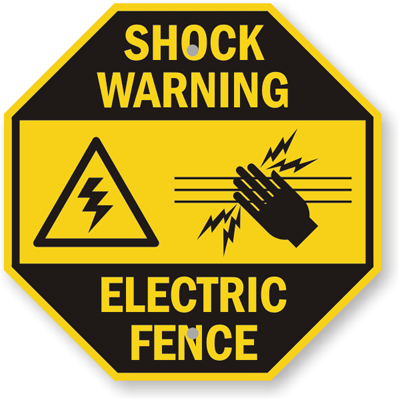




1. **Physical Controls:**

**PHYSICAL – DETERRENT – WARNING SIGNS:**

**DESCRIPTION:** Warning signs are an excellent deterrent for unauthorized access; if you simply put a sign up that warns people of electric fences, guard dogs or security on the premises it will help deter unauthorized access to the facility. Any sign that warns would-be intruders not to enter the premises could be classified as a physical deterrent. Security guards or guard dogs can also be classified as physical deterrents, since simply seeing them out on the premises can deter unauthorized access to the facility. I am including two images of warning signs that are typically used to warn/deter people from accessing unauthorized areas.



**PHYSICAL – PREVENTATIVE – FENCES:**

**DESCRIPTION:** Fences are used to prevent unauthorized access to a facility by barring off certain entry points. Fences can also be electrified or have barbed wire on top, and these are both commonly used in high-security areas to protect the premises from unauthorized access. Fences may be used with things like landscaping, CCTV cameras and security guards to create the concept of layered defense in a business. I have included a picture of a typical electric fence that may be used in high-security areas.



**PHYSICAL – DETECTIVE – CCTV:**

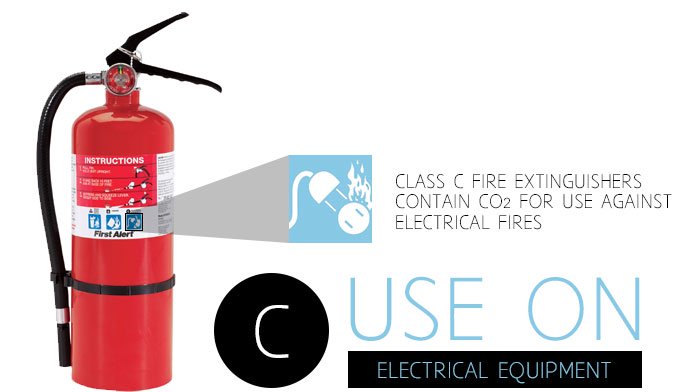
**DESCRIPTION:** CCTV cameras are used to protect both the outside and the inside of the premises. This is a detective type of access control because it is used to identify an incident visually, so they can be used as an important layer of defense. CCTV cameras can also be classified as deterrent or compensating access controls, since they both discourage incidents from occurring while also providing an alternative form of control over employees for management. Below I have provided an image of a normal CCTV monitoring room above an image of what most common CCTV cameras in use tend to look like.





**PHYSICAL – CORRECTIVE – FIRE EXTINGUISHER:**

**DESCRIPTION:** Fire extinguishers are used if a fire breaks out in the office; an employee can grab this device and snuff the fire out with chemicals. Different fire extinguishers are used for different types of fires, so it is important to theorize about what fires could erupt in the workplace before purchasing a fire extinguisher. There are three classes for fire extinguishers – they are either class A, B or C; the class given to the extinguisher is based on what type of fire they can fight the best. A class A fire extinguisher is used to fight trash/wood/paper fires, a class B fire extinguisher is used to fight liquid fires (such as cooking liquids, gasoline, kerosene, etc.) and a class C fire extinguisher is used to fight electrical fires. The most suitable extinguisher for an IT department would be a class C fire extinguisher (which is also the most common type of extinguisher), and I have included a picture of what these typically look like below.



**PHYSICAL – RECOVERY – RECONSTRUCTION:**

**DESCRIPTION:** If the business is physically attacked and a portion of the building is damaged/destroyed, reconstruction is the recovery plan to go with. Reconstruction will help restore the business back to working conditions (if the physical damage was enough to originally obstruct working conditions). If the physical damage to the building is too much to repair through reconstruction (i.e., damage caused from natural disasters) then the building may have to be rebuilt completely. If this happens, the employees will have to be relocated to a hot/warm site to continue business operations while the business is being rebuilt. I have attached a picture of what typical business reconstruction looks like after a natural disaster.



**PHYSICAL – COMPENSATING – LAYERED DEFENSE:**

**DESCRIPTION:** Layered defense is the act of creating boundaries and barriers in order to defend an area from incoming threats. Layered defense can be done by creating a blueprint of the area and mapping out the most important things to defend; this can be servers, money/e-funds, or any important equipment that needs to be protected. Some common ways of doing this involve using barbed wire fences, landscaping (such as trees, shrubs, etc.), gates, bollards (for providing security from vehicles damaging property) and applying some of the other physical access controls listed here. When these concepts are applied, the layered defense system will prevent unwanted intrusions by making every physical access control useful for barring access (i.e., the layered defense system compensates for the partial defense that each individual access control provides). The model I am including with this description is the common layered defense model used in most workplaces.

