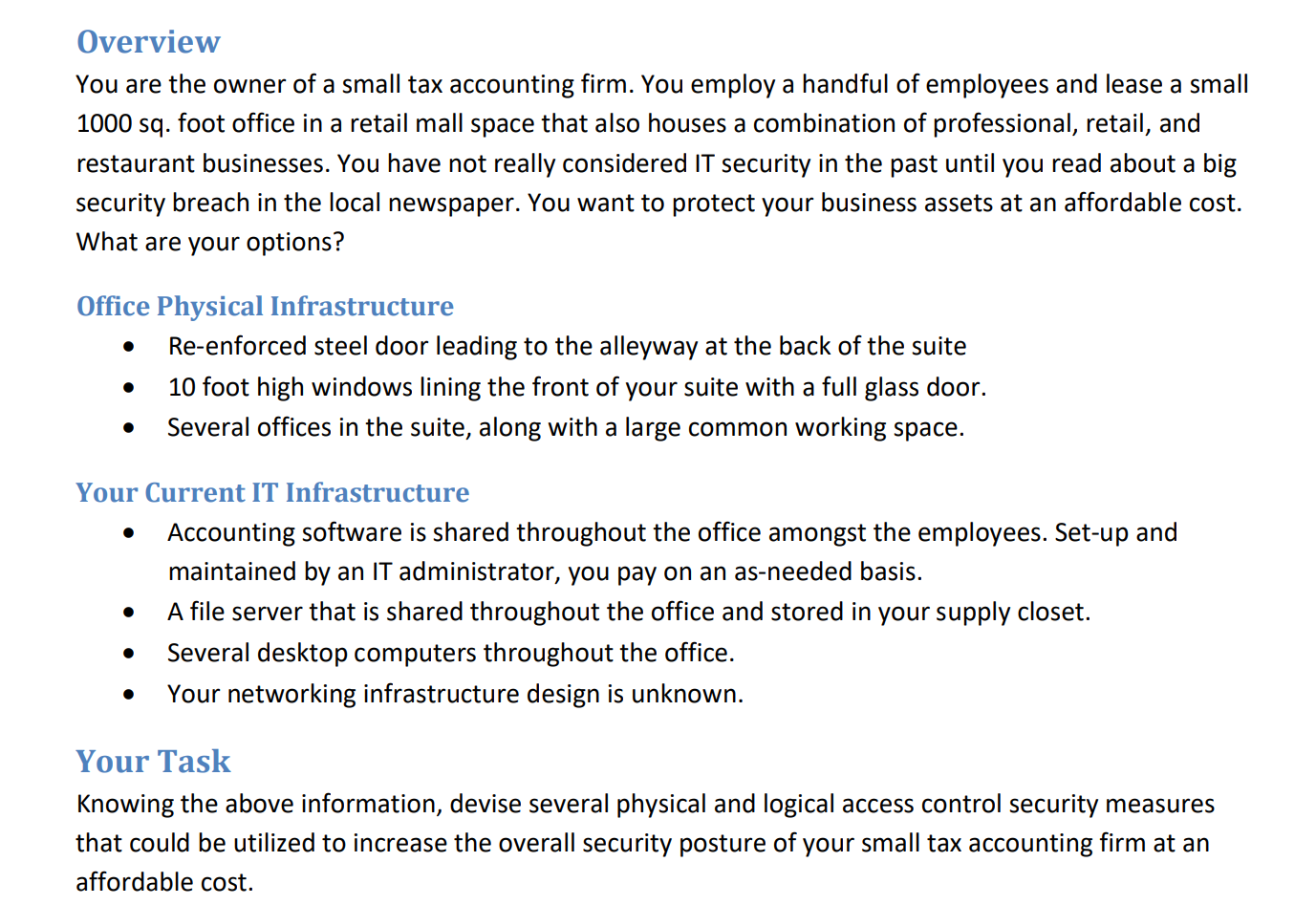
|  |  |
| --- | --- |
| Course | Information Security |
| Assignment | Assignment 4- Physical & Logical Access Controls |
| Student ID | 100899259 |
| Student Name | Maisha Khatoon |

**InfoSec Assignment 4**

**Physical & Logical access controls**



|  |  |
| --- | --- |
| **Physical Security Access Control Ideas** | **Logical Security Access Control Ideas** |
| Security Guards | Password Policies |
| Proximity Cards | Access Control Lists (ACLs) |
| Video Cameras | Device Policy |
| Mantrap | Multi-factor Authentication |
| Door Access Systems | Antivirus and security patch updates |

Write two paragraphs highlighting the pros of the access controls you have selected and why the controls are sufficient in addressing the security concerns. One paragraph will be geared toward physical controls, the next will be geared toward the logical controls and best practices that go along with the logical controls.

**Physical Access Controls:**

Combining physical security access restrictions can help a small tax accounting firm protect the privacy of its clients, workers, and sensitive data. Some access controls and their benefits are as follows:

* Security personnel: Security personnel can fend off potential dangers and make themselves physically present to bar unlawful entry. They can keep an eye on the area, react to accidents, and help when necessary. Both the company's clients and employees may feel more secure as a result.
* Proximity Cards: Only authorized staff may enter parts of the company using proximity cards. The cards can be disabled if they are lost or stolen and are designed to grant access to only certain locations. This may aid in limiting illegal access to confidential parts of the company.
* Video cameras: Video cameras can record any issues that happen as well as a visual record of who enters and leaves the premises. In the event of an incident, this can help identify potential risks and give proof.
* One person may only enter or leave a secure location at a time using a mantrap, a type of physical access control system. This can stop unauthorized entry and lessen the chance of tailgating, which happens when an unauthorized person follows a person who has access.
* Door Access Systems: Door access systems can limit authorized personnel's access to specific regions of the company. The system can be configured to permit access to only certain locations, and it can be turned off if the card or key is misplaced or stolen. This may aid in limiting illegal access to confidential parts of the company.

In conclusion, a small tax accounting firm’s security problem can be fully addressed by a mix of physical security access controls, such as security guards, proximity cards, video cameras, mantraps, and door access systems. These safeguards can aid in preventing unwanted access, thwarting potential threats, and creating a secure environment for the firm's staff and clients.

**Logical Access Controls:**

A small tax accountancy firm's sensitive data must be shielded from cyber attacks by logical security access controls. Some access controls and their benefits are as follows:

* Password Policies: Password policies can ensure that staff members create strong, secure passwords that are challenging for hackers to brute-force or guess. To avoid the use of outdated or hacked passwords, they can also mandate regular password changes.
* Access Control Lists (ACLs): ACLs allow only authorized users to access specific files, directories, or applications. This can lessen the impact of a cyber attack and help prevent unauthorized access to critical information.
* Device Policy: Device policy can make it mandatory to only use devices that have been certified by the firm and which adhere to particular security standards, such as encryption and antivirus software. This might restrict the usage of unsecured devices that might jeopardize the information security of the company.
* Multi-factor Authentication: By asking users to provide additional authentication elements, like a fingerprint or a code sent to their mobile device, MFA can increase the security of the login process. Even if the password is compromised, this can stop illegal access.
* Updates to antivirus software and security patches can help safeguard the company's data against malware and other online threats. They can identify and eliminate harmful software and vulnerabilities that hackers might use.

In conclusion, a small tax accounting firm's security concerns can be addressed comprehensively by combining logical security access controls including password policies, ACLs, device policy, MFA, and antivirus and security patch updates. These safeguards can maintain the confidentiality, integrity, and accessibility of the company's information while also assisting in the prevention of cyber risks and mitigating harm in the event of an attack.