Information Security

Why is it important?

* Information is valuable
* Information is personal

What information is covered?

* Personal
* Legal
* Corporate
* Operational Data

If its not in the public domain protect it!!

Risks and consequences of not protecting

* The data’s value
* The added risk of a direct attack (on people or systems)
* The cost of regulatory fines
* The cost of restoring or recreating what was lost
* Reputational damage

When it goes wrong: (eg)

* Hiv clinics accidentally leaks patient details
* Bank fines for 500k for data loss
* Big losses

Why do security breaches occur:

* Ignorance of the rules (policy violations caused by a lack of training)
* Failing to realize that the data was confidential
* Insufficient methods to protect data
* Deliberate leaks
* User error

Understanding the data universe :

Data classification system

Lifecycle

Creation => Storage/retrieval (use) => Disposal

Classifying information:

Confidential

Inside

Internal

Public

Security in the clouds   
Avoid content dumps: copying everything as a backup “just in case”

Conduct due diligence before granting shared access

DO NOT Allow shared logins

Create new folders to give other people data

Good policies for info security

Providing information and training

Carrying out regular risk assessments

Testing if our systems are secure

Providing appropriate tech to keep info safe

Appointing people with specific responsibilities for information security

Requiring everyone to read and implement the information security policy

| **Physical securities** | **Logical securities** |
| --- | --- |
| Trained security personnel | Strengthened passwords |
| Trained animals | Firewalls |
| Strengthened Boundaries | antivirus |
| Visitors have special clearance with accompaniment | Proxy servers |
| Keep sensitive rooms where normal people cannot have easy access | Use VPNs |
| Strengthened locks | Use a trusted Cloud source for data backups and storage |
| Different security Levels of key cards | Use encryption in data |
| Have protection against natural disasters | Use 2 factor authentication |
| Have surge protectors |  |
| Have a backup power source in case of a power outage where you need to access the systems frequently |  |

Critical characteristics of information

The value of information comes from the characteristics it possesses:

* Availability
* Accuracy
* Authenticity
* Confidentiality
* Integrity
* Utility
* Possession

International standards of the data security

Framework: COBIT19