**Module 5 Risk Management**

**5.8 Data Privacy**

**Data Sensitivity Labelling & Handling**

* Data/information classified according to its value & level of sensitivity
* Appropriate level of security can be applied
* Process should be

1. Easy to apply
2. Consistent
3. Visible

**Data Sensitivity Classifications**

* Common labels

1. Public/unclassified – no harm if disclosed
2. Confidential – limited harm if disclosed
3. Secret – grave harm if disclosed
4. Proprietary – limited to internal use only (restricted externally)
5. Private – information regarding people

* Classification terms & labelling determined by organisation

**Sensitive Data Types – Legal**

* PII (Personally Identifiable Information)

1. Data that identifies/traceable to specific individual
2. Name, Social Security Number, Biometrics, Address
3. See NIST SP800-122

* PHI (Protected/Personal Health Information)

1. HIPAA – any information about health status/provision/healthcare/payments for healthcare that is created/collected by “Covered Entity” that can be linked to specific individual

**Data Roles**

* Data owner
* Data custodian
* Privacy officer

**Data Retention & Disposal**

* Retention

1. US Federal Rules of Civil Procedure (FRCP)
2. Keep information only as long as you need it & no longer
3. Set in Data Protection Policy

* Disposal - properly disposing data & associated hardware

**Data Destruction & Media Sanitisation**

* Trusting 3rd parties for destruction
* Observe destruction process
* Transportation to destruction facility
* Use of media after destruction
* Best practice to combine method
* Burning

1. Use heat/fire
2. Not environmentally friendly

* Shredding

1. Reduces size of objects with intent of making them un-usable
2. Items may still be reassembled

* Pulping

1. Reduces paper to liquid slurry
2. Can then be safely recycled

* Pulverising

1. Using hydraulic/pneumatic action to reduce materials to loose fibres & shards
2. Costly

* Degaussing – using large magnet to remove data from magnetic storage media (Eg. Hard drives & magnetic tapes)
* Purging

1. Removing files & all traces of data
2. Sanitisation

* Wiping

1. Overwriting data
2. Data replaced (often with random 0’s & 1’s) & then removed