Data Security Unit:
End of Block – Outcome 4 check

- Defining what data is and defining a security breach (remembering, viewing of data without consent / permissions is a data security breach as well as the extraction or editing of data)
- Levels of risk and personal risk as well as businesses
- Legislation: GDPR (rights of the individual, consent, controller, processor, accountability, the ICO, punishment, financial punishment), Human Rights Act, FOI, Misuse of Computers Act, Copyright and Patents Act, other legislation such as terrorism etc.
- Implications of security breaches upon individuals and organisations (the risks, the punishment, the implications such as reputation etc.)

- Password Management and policies (character length, time periods, complexity, use of symbols and numbers etc.). Password Managers and users being able to remember, especially if changing passwords on a regular basis.
- Encryption: Explaining what encryption is, why it is needed, data at rest, storage of passwords, digital rights management, file or folder encryption, data in transit, devices with encryption, VPN, digital certificates, certification authorities, protocols such as https, public / private keys explanation, TSL/SSL/protocols)
- Firewalls: What a Firewall does, how it works.
- Intrusion Detection Systems
- Access Control and Permissions

- Physical security: protection of personnel, hardware, software, networks, data, including fire, flood, vandalism, terrorism and other emergencies.
- Brute force attacks, physical access control, surveillance systems, testing of security systems.
- Physical methods for restricting access: locks, protecting routers / servers / hardware, card entry, biometrics, security staff, CCTV, alarms, protecting cables and cabinets.
- Firewall configuration: Blacklist and Whitelisting, pros and cons of each, blocking specific activity or websites, use of firewall configuration for security.
- Data Backup: Full, Incremental, Differential
- Backup and Recovery planning: timescales, frequency of backing up, testing of backup data and recovery testing. Place of backup storage: On-site or off-site or cloud. Media options such as disc, other media, cloud.
- Recovery: recovery plan. Responsibilities, planning for disasters, timescales, training staff, PSU Power Supply Units, UPS Uninterruptible Power Supply, RAID Redundant Array of Independent Disks) and different levels of RAID.

- Security Strategy: creating a policy, a plan, addressing the risks, managing the risks.
- Appointing a Chief Officer for Security, ensuring compliance, investigations such as digital forensics and risk management by appointing someone responsible.
- CIA triad (Confidentiality, Integrity, Availability)
- Review of security strategy annually and longer-term approaches.

Lecturer: Mark Gillan