|  |  |
| --- | --- |
| Analyse |  |
| Recover |  |
| Manage |  |
| Respond |  |
| Investigate |  |

|  |  |
| --- | --- |
| Who is responsible for what |  |
| Staff do’s & don’ts |  |
| Defining back up process | 1.  2.  3. |
| Timeline for data recovery |  |
| Location of alternative provision |  |

**Disaster recovery policy**

**Action to take after an attack**

|  |  |
| --- | --- |
|  | Why important? |
| Password policy |  |
| Acceptable installation / use policy |  |
| Parameters for device hardening |  |

**B3 Policy**

**Defining security parameters**

|  |  |
| --- | --- |
|  | Why important? |
| Who is responsible for what |  |
| How to report concerns |  |
| Reporting to staff/ employees |  |

**Defining responsibilities**

|  |  |
| --- | --- |
| Penetration testing |  |
| Analysis of system data or behaviours to identify potential risks |  |
| Ethical hacking | 1.  2. |

**Finding weaknesses & improving system security**

**User Access Restriction**

**Data level protection**

|  |  |
| --- | --- |
| Firewall | 1.  2. |
| Software /Interface design | 1.  2.  3. |
| Anti-virus software |  |
| Device hardening |  |
| Backup & recovery procedures |  |
| Encryption of shared data | 1.  2. |
| Encryption of transmitted data |  |

**BTEC DIT**

**B Cyber Security**

|  |  |
| --- | --- |
| Physical |  |
| Passwords |  |
| Correct settings / levels of access |  |
| Biometrics |  |
| Two factor authentication | 1.  2.  3. |

**B2 Prevention and Management of threats to data**