|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Learner Name:** |  | **Assessor:** | |  |
| **Centre Name:** |  | **Internal Verifier (if applicable):** | |  |
| **BCS ID / ULN:** |  |  | |  |
| **Unit Information Summary** | | | | |
| **Approximate Guided Learning Hours: 20** | | | **Unit Number: D/502/4258** | |
| **QCF Credit Value: 3** | | | **Learning Outcomes (Number): 1** | |
| **Examples of Context:**   * Develop backup and security guidelines for others to follow. * Setting up a backup and recovery plan for a small business running a peer to peer network. * In larger organisations, aspects relating to security policy and practice at Level 3 may be the responsibility of IT professionals. | | | **Learning Materials Available:**  None for this unit | |
| **Suggested Assessment Methods:**  All ITQ units may be assessed using any method or combination of methods which clearly demonstrates that the learning outcomes and assessment criteria have been fully met   * Scenario * Coursework * Portfolio of Evidence – classroom or work-based * Practical Demonstration * Assignment * Task-based Controlled Assessment * Professional Discussion * Observation * Witness Statement | | |

| **Ofqual Learning Outcome** | | **Assessment Criteria** | **Examples of Content**  *The examples given are indicative of the learning content at each level and are not intended to form a prescriptive list for the purpose of assessment* | **Evidence Location** |
| --- | --- | --- | --- | --- |
| **1 Select, use and develop appropriate procedures to monitor and minimise security risk to IT systems and data** | 1.1 | Evaluate the security issues that may threaten system performance | *Threats to system performance: Unwanted e-mail (often referred to as “spam”), malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers) and hackers; hoaxes; vulnerability* |  |
| 1.2 | Select, use and evaluate a range of security precautions to protect IT systems and monitor security | *Security precautions: Use access controls. Configure anti-virus software, adjust firewall settings, adjust internet security settings; carry out security checks, report security threats or breaches; backup; store personal data and software safely; treat messages, files, software and attachments from unknown sources with caution; proxy servers; download security software patches and updates; effectiveness of security measures* |  |
| 1.3 | Evaluate the threats to system and information security and integrity | *Threats to information security: From theft, unauthorised access, accidental file deletion, use of removable storage media; malicious programs (including viruses, worms, trojans, spyware, adware and rogue diallers), hackers, phishing and identity theft; unsecured and public networks, default passwords and settings, wireless networks, Bluetooth, portable and USB devices* |  |
| 1.4 | Manage access to information sources securely to maintain confidentiality, integrity and availability of information | *Access to information sources: Username and password/PIN selection and management, online identity/profiles; Respect confidentiality, avoid inappropriate disclosure of information; digital signatures; data encryption; security classification, preserve availability* |  |
| 1.5 | Explain why and how to minimise security risks to hardware, software and data for different users | *Minimise risk: Access controls: Physical controls, locks, passwords, access levels, data protection, data retention. Security measures: anti-virus software, firewalls, security software and settings. Risk assessment: anti-spam software, software updates; risk management; user profiles, operating system settings, user authentication (ID cards, smart cards, biometrics); risks associated with widespread use of technology* |  |
| 1.6 | Apply, maintain and develop guidelines and procedures for the secure use of IT | *Security guidelines and procedures: Set by: employer or organisation, privacy, laws and regulations, disaster recovery plans, contingency systems, dealing with security breaches, backup procedures; administrative procedures and controls* |  |
| 1.7 | Select and use effective backup and archiving procedures for systems and data |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessment Report** | | | | |
| **Assessor feedback / comments** (continue on additional sheet / assessment report if necessary) | | | | |
| **Internal Verifier actions / comments / feedback** | | | | |
| **Assessor signature:** |  | **Assessment date:** |  | **Reason for IV:**  **New Assessor**  **Random Sample**  **New Unit/Qualification**  **Other** |
| **IV signature:** |  | **IV date:** |  |