

Name:

BTEC IT Extended Certificate – Unit 2 Content and Revision List



A) Cyber security threats, system vulnerabilities and security protection methods

A1 Cyber security threats			
<i>Students should apply their knowledge and understanding of the function and impact of internal and external threats</i>			
Content			Revised
	Internal threats:		
	employee sabotage, deliberate and accidental		
	• Theft or loss of ○ Physical equipment ○ Data ○ Software/licences • use of unauthorised software ○ license and legal liability issues ○ compatibility issues ○ interference with running of the network/other software ○ used for spying, harassment, illegal activities ○ used to avoid/interfere with monitoring, auditing, user/device supervision		
	Accidental or deliberate damage		
	• fire • flood • Power loss • terrorism • Other disasters		
	Weak cyber security measures and unsafe practices		
	• Security of computer equipment and storage devices • Security vetting of visitors • Visiting untrustworthy websites		
	Accidental loss or disclosure of data/credentials		
	• human factors ○ negligence ○ poor training ○ not following security procedures • inadequate monitoring and reporting • weak security culture		
	Function of External threats		
	Malicious software (malware)		
	• viruses ○ boot sector ○ web script ○ macro ○ worm ○ rootkit ○ trojan ○ browser hijack		

		○ polymorphic		
		• spyware		
		○ keylogger/data thief		
		○ system monitor		
		○ mobile device tracker/stalkerware		
		○ web beacons and tracking cookies		
		• adware		
		○ potentially unwanted program (PUP)		
		○ legitimate adware		
		○ abusive or deceptive adware, legal and illegal		
		• ransomware		
		○ encryptors		
		○ lockers		
		○ scareware		
		○ leakware/doxware		
		• bots		
		Hacking – commercial, government, individuals		
		• Denial of Service (DoS) and Distributed Denial of Service (DDoS)		
		• browser hijack		
		• cyberwarfare		
		• data theft		
		• data tampering		
		○ back end – databases and other data stores		
		○ front end – web pages and other public facing displays		
		Sabotage – commercial, government, individuals, terrorism		
		• data poisoning		
		• data tampering		
		• data destruction		
		• fakes		
		○ images, video, audio, documents		
		○ using manual/traditional software methods		
		○ using Artificial Intelligence (AI)		
		• damage to/hijacking of		
		○ machinery		
		○ vehicles		
		○ internet connected devices		
		○ industrial processes		
		○ critical infrastructure – commercial and national		
		Social-engineering techniques used to obtain secure information by deception		
		• phishing, vishing, smishing		
		• whaling, spear phishing		
		• Domain Name System (DNS) spoofing		
		• pretexting/impersonation		
		Physical security		
		• unauthorised access to secure areas		
		○ tailgating		
		○ forced entry		
		○ impersonation		
		○ coercion		

		unauthorised access to devices		
		o unattended devices		
		o shoulder surfing		
		o theft of device		
		o lost devices		
		o devices/interfaces installed in public areas		
		Impact of a credible threat, likely to result in some form of loss:		
		operational loss		
		manufacturing output		
		service availability		
		data availability		
		financial loss		
		organisational		
		o cash flow problems		
		o loss of profits		
		o increased insurance costs		
		compensation		
		o refunds to customers		
		o payments for compromising customer data/personal information		
		o costs of remedial actions such as credit score/identity protection		
		o payment for contractual default/inability to provide contracted service/goods		
		o discounts/write-offs to retain/regain customers		
		legal liability		
		o fines		
		o penalty payments		
		o costs of statutory requirements in investigations		
		o legal fees		
		reputational loss		
		loss of trust		
		poor customer reviews		
		o on social media		
		o on review websites		
		o on organisation's own website		
		intellectual property loss		
		new product design		
		testing and development data		
		organisational strategy		
		trade secrets		
		Cyber security threats vary over time and cyber security organisations provide regular updates on the current and changing threat landscape.		
		National Cyber Security Centre (NCSC) UK		
		latest threat reports and malware analysis		
		news (reports and advisories on recent activity)		
		National Institute of Standards and Technology (NIST) USA		
		news (reports and advisories on recent activity)		
		Open Web Application Security Project (OWASP)		
		OWASP Top 10		

A2 System vulnerabilities

Students should apply their knowledge and understanding of the different types of systems and their vulnerabilities, tools to assess the vulnerabilities and the risk management measures.

Content		Revised	
	Vulnerabilities of different types of computer and/or systems and the different threats they are exposed to.		
	Network		
	▪ firewall ports		
	○ types		
	assigned/well known, such as port 80 for Hypertext Transfer Protocol (HTTP)		
	registered, used by operating systems, internet services and specific pieces of software		
	dynamic/private, used for private/customised services, temporary needs		
	○ vulnerabilities		
	open ports		
	spoofing		
	Denial of Service (DoS)		
	▪ external storage devices		
	○ universal serial bus (USB)/flash drive		
	○ SD card		
	○ external hard drive		
	○ solid state device (SSD)		
	○ optical disk and magnetic tape, in the context of backup systems		
	Organisational		
	▪ permissions or privileges		
	○ read, write, execute, modify/change		
	○ user, administrator, system, group		
	○ on files, folders/directories, devices, data structures, services		
	▪ password policy		
	○ minimum and maximum length		
	○ character restrictions		
	○ frequency of password reuse		
	○ disallow personal names, birthdays etc		
	○ specify a minimum password age		
	○ prevent password sharing/multiple logon with same password		
	▪ password management		
	○ password managers		
	on an individual device		
	synchronised between devices		
	cloud based		
	to generate passwords		
	○ lockout of inactive accounts		
	○ effective new user/leaving user process		
	○ auto-filling of forms/screens by		
	browser		
	dedicated software		
	Software		
	• from an untrustworthy source		
	• software downloads		

		○ requirement for		
		trusted source		
		Hypertext Transfer Protocol Secure (HTTPS) or lock symbol		
		malware scan, pre-install		
		hash check		
		○ malicious/deceptive installers		
		• illegal copies		
		○ lack of security support/updates		
		○ backdoors		
		○ containing malware		
		• zero-day exploits		
		○ new threats		
		○ window of exploitation before fix/patch applied		
		• data storage and processing software		
		○ SQL injection		
		○ poor/no protection on internet-facing data systems		
		○ design/security flaws in web interfaces		
		• missing patches/updates		
		Operating system, Graphical User Interface (GUI) and Command Line Interface (CLI)		
		• unsupported/out of support versions		
		• missing patches/updates		
		• missing/incorrect security settings		
		Mobile devices reliant on Original Equipment Manufacturers (OEMs) to update system software		
		Physical		
		• theft of equipment/devices containing sensitive data		
		• mobile device		
		• data storage device		
		• poor/missing security for restricted areas		
		Process of how people use the system		
		• leaks, intentional and accidenta		
		• sharing security details		
		• flawed security processes		
		Security implications of cloud computing and of the Internet of Things (IoT) devices		
		• Cloud computing		
		○ missing/incorrect/default security settings		
		○ third party/cloud provider access		
		○ reliant on third party security		
		○ data movement outside of the organisation's network/over the internet, risk of interception/theft/tampering		
		• IoT		
		○ weak/no encryption on IoT devices/transmissions		
		○ default passwords		
		○ lack of patches and updates		
		○ deployment by non-IT staff		
		○ flawed/insecure control interfaces		
		○ poor/no compatibility with network security systems		
		○ eavesdropping/smart devices always listening/sending voice data		

	Where to find up-to-date sources of information on specific known hardware and software vulnerabilities		
	manufacturer's website		
	forum/technical help website for IT professionals/cyber security specialists		
	third party websites specialising in specific hardware or software		
	Attack vectors		
	Wireless		
	• Wi-Fi, IEEE 802.11 family of standards		
	• Bluetooth		
	• Cellular		
	• satellite link		
	• Infra Red (IR)		
	• Near-field communication (NFC)		
	• Radio-frequency identification (RFID)		
	Internet connection		
	• types ○ copper cable ○ optical fibre ○ Wi-Fi ○ cellular/5G • connection devices ○ modem/router-modem, cable and optical fibre ○ wireless router ○ cellular device/5G router		
	Internal network access devices		
	• router		
	• switch		
	• wireless access point		
	Types and uses of tools and methods to assess the vulnerabilities in computer systems		
	port scanner		
	network mapper/system discovery		
	registry checker		
	website vulnerability scanner		
	vulnerability detection and management software		
	assessing user vulnerabilities		
	Use of independent third-party review of a system and network designs before implementation		
	establishing due diligence		
	third party certification		
	Applications and features of penetration testing for common threats, those in the Open Web Application Security Project (OWASP) top 10.		
	uses range of techniques to find weak spots		
	checks against lists of known vulnerabilities		
	produce reports, in appropriate formats		
	Passive risk management measures		
	risk transfer to a third party (commissioning a service provider)		
	risk avoidance by stopping an activity		
	risk acceptance		

A3 Legal responsibilities

Students should know the responsibilities in relation to current legal legislation

Content		Revised	
Current legislation			
	General Data Protection Regulation (GDPR) (requirements for protection of data, privacy rights)		
	Computer Misuse Act 1990 (protects personal data held by organisations from unauthorised access and modification)		
Areas the legislation applies to			
	protection of data, in storage and when transferred		
	privacy, personally identifying information (PII)		
	unauthorised access to computers/devices		
	unauthorised access to and modification of data		
Legal responsibilities legislation			
	General Data Protection Regulation (GDPR)		
	- principles - lawfulness - fairness and transparency - limited to stated purpose(es) - accuracy - keep minimum amount of data - store for minimum amount of time - maintain confidentiality and integrity - legal reasons for data processing - consent - contractual obligation - legitimate interest - vital interest - legal requirement - public interest - personal rights, people have the right to: - access their own personal data - be informed about how and why their data is used - have their data corrected, removed or restricted - object to the data being used - portability (have data supplied in a machine readable format) - not to be subject to a decision based solely on automated processing.		
Computer Misuse Act			
	Responsibilities of organisations – exercise due care to comply with its security obligations under GDPR		

A4 Software and hardware security measures

Students should apply their knowledge and understanding of the use and effectiveness of security measures for software and hardware, use of encryption and precautions to protect wireless local area network (WLAN)

Content		Revised	
	Software and hardware		
	physical security measures		
	• site security locks		
	○ mechanical		
	○ electronic		
	○ network connected		
	• card entry		
	○ Near-field Communication (NFC)		
	○ Radio-frequency Identification (RFID)		
	○ barcode, QR code		
	○ magnetic stripe		
	○ embedded microprocessor/chip		
	• biometrics		
	○ fingerprint		
	○ iris/retina/eye pattern		
	○ facial recognition		
	○ voice recognition		
	○ handwriting/signature/pattern, etc. – on touchscreen/pad		
	• Closed-Circuit Television (CCTV)		
	• security staff		
	• alarms – on buildings/restricted areas and on devices		
	• protected cabling and cabinets		
	• staff training		
	data storage, data protection and backup, and recovery procedures		
	• backup types		
	○ full		
	○ differential		
	○ incremental		
	• backup strategies		
	○ onsite, offsite, cloud		
	○ automated, manual		
	○ hot site, warm site		
	• redundant array of independent disks (RAID) vs backup		
	• archiving vs backup		
	• data resilience		
	• recovery types		
	○ file/data restore		
	○ image restore of; disc, device, system		
	○ full/bare-metal restore		

		antivirus software and detection techniques		
		• virus signatures, scanning		
		• heuristics techniques used to identify potentially suspicious file content or behaviour		
		• file integrity check, checksum		
		• techniques for dealing with identified threats		
		○ warning		
		○ logging		
		○ prevent execution		
		○ quarantine		
		○ deletion		
		software and hardware firewalls and the filtering techniques they use		
		• packet filtering and inspection		
		• application layer awareness		
		• inbound and outbound rules		
		• network address		
		user authentication		
		• user login procedures		
		• strong password, password policy compliance		
		• biometric authentication		
		• single factor and multi-factor authentication (MFA)		
		○ knowledge/things you know		
		○ possession/things you have		
		○ inherence/things you are		
		○ location factors such as IP address, MAC address, global positioning system (GPS) location		
		○ behaviour factors such as how a signature/pattern is made, how a keyboard is used		
		• security tokens		
		○ connected such as a Universal Serial Bus (USB) key, or smartcard plus reader		
		○ contactless such as a Bluetooth enabled dongle		
		○ disconnected, a device that generates a code independently such as:		
		○ a smartphone with a security app		
		○ a dedicated device issued by a bank or credit card company		
		• Kerberos network authentication for Windows® and Linux®-based operating systems		
		• basic key exchange process		
		○ client request		
		○ server response		
		○ authentication of server response		
		○ key exchange		
		• certificate-based authentication		
		○ Transport Layer Security (TLS)		
		○ Secure Sockets Layer (SSL)		
		○ client/device certificate		
		○ Public Key Infrastructure (PKI)		

		○ Certificate Authority (CA)		
		○ self-signed certificate		
		access controls and the methods to restrict users' access to resources		
		• Discretionary Access Control (DAC), users have control of their own files and resources		
		• Role-Based Access Control (RBAC), administrator sets rules groups of users based on their role in an organisation		
		• Rule-Based Access Control (RBAC), administrator sets rules for individual users		
		• resources		
		○ applications		
		○ folders		
		○ files		
		○ data sets		
		○ physical resources/devices		
		trusted computing		
		• benefits, increased security		
		• drawbacks, loss of user control/privacy/anonymity		
		Finding lost or stolen devices		
		• device location technology		
		○ Global Positioning System (GPS)		
		○ phone home on connection		
		○ device tracking and location reporting software		
		Device based security		
		• timed lockout of desktop/screen		
		• desktop/screen lock after failed login attempts		
		• memory wipe/factory reset after failed login attempts		
		• remote access for lock/wipe/reset of lost/stolen device		
		Use of encryption		
		storage encryption		
		• safe password storage		
		• Digital Rights Management (DRM)		
		• file, folder, disc, device encryption		
		communications encryption		
		• symmetric encryption		
		○ secret key		
		○ Advanced Encryption Standard (AES)		
		• asymmetric encryption		
		○ public and private keys		
		○ Rivest–Shamir–Adleman (RSA)		
		○ Diffie–Hellman key exchange		
		• integrated into smart, mobile and built-in/embedded devices		
		• The Onion Router (TOR)		
		• Virtual Private Networks (VPNs)		
		• digital certificates and certificate authorities		
		• Hypertext Transfer Protocol Secure (HTTPS)		
		• public/private keys		

		• End-to-End Encryption (E2EE)		
		• secure message apps		
		Precautions that can be taken to protect a Wireless Local Area Network (WLAN) from unauthorised access:		
		Media Access Control (MAC) address filtering and hiding the Service Set Identifier (SSID)		
		wireless encryption		
		• Wi-Fi Protected Access 2 and 3 (WPA2/3)		
		• Wi-Fi Protected Setup		
		• known wireless vulnerabilities		
		○ unsecured access point		
		○ piggybacking/unauthorised use of unsecured network		
		○ Evil Twin attack/fake access point		
		○ wireless sniffing/eavesdropping		
		• mitigation methods for attacks on Wi-Fi		
		○ changing default passwords/settings/names		
		○ use of block and allow lists for device access		
		○ use of VPNs		
		○ use of WPA2/3		
		○ firewalls		
		Security issues during network and system design to ensure security is built		
		expect attacks to happen and plan for them		
		design the system to run on 'fewest privileges'		
		assume everyone will get access to the system design		
		avoid reliance on secrecy/obscurity		
		compliance with information security standards such as ISO 27000		

Name:

BTEC IT Extended Certificate – Unit 2 Content and Revision List



B) Use of networking architectures and principles for security

Students should apply their knowledge and understanding of the security issues of networked systems and how to secure them in organisational contexts. Students should be able to interpret and amend schematic diagrams.

B1 Network types			
Content			Revised
Applications and features of networks:			
Network types			
• Local Area Network (LAN)			
• Wireless Local Area Network (WLAN)			
• Wide Area Network (WAN)			
• Storage Area Network (SAN)			
• Personal Area Network (PAN)			
• the internet			
Private network types			
• intranet			
• extranet			
• cloud network			
wired and wireless integration			
• ethernet standards for wired and wireless (802 family)			
• compatibility/interoperability issues such as protocols and access points			
• admin issues such as channels and IP addresses			
• technical issues such as signal strength and interference			
schematic diagrams			
• network diagram, logical and physical			
• diagrams showing specific items such as port numbers or network addresses			
Features/requirements of networks (cyber security related)			
• scalability			
• software and hardware sharing/compatibility			
• data and file sharing/transfer			
• performance/response time			
• backup management			
• security settings			
• reliability			
• fault tolerance			
• communications			
Applications and features of network topologies:			
physical topologies			
• star			
• extended star			
• hierarchical			
• wireless mesh			

	ad-hoc (mix of wired and wireless for Bring Your Own Device (BYOD))		
	logical topologies		
	logical bus		
	logical ring		
	network architecture		
	peer-to-peer		
	client/server		
	thin client		
	modern trends – applications and security issues of:		
	virtualisation		
	segmentation		
	isolation/sandboxing/containerisation		
	reduced attack surface		
	Cloud computing		
	configuration issues, default access settings		
	reliance on service provider, data leaks/loss/theft		
	Application Programming Interfaces (API), vulnerabilities in interface to cloud services/storage		
	account hijacking		
	BYOD		
	- issues with organisational data on a private device - data security, on device and when transferred - patches, maintenance, updates, compatibility - organisational v personal applications - erasing/wiping data after use/when no longer required - tracing/auditing data use/movement		
	- Software-Defined Networking (SDN) - segmentation - remote management - automation - scalability - reduced hardware requirements		
	- Storage Area Network (SAN) - redundancy - scalability - access controls - encryption/digital certificates		
	- Internet of Things (IoT) - Application Program Interface (API) security issues - default passwords/security settings - lack of patches/updates - Zigbee, Bluetooth 5 and similar low-power wireless technology - mesh capability - ease of interception/interference - range issues - botnets - spying via networked cameras/smart hubs/TVs - exposure of non-traditional networked devices such as medical equipment, home appliances, commercial machinery, and vehicles		

	• remote working		
	○ devices seen/used by others such as family members, visitors		
	○ need for VPN/encrypted link		
	○ security of home network/Wi-Fi		
	○ weaknesses of/reliance on third party communication systems such as video calls		
	○ issues around data storage/transfer/use of the cloud		

B2 Network components			
Content			Revised
	Application and features of hardware components:		
	end-user devices, with connectivity and processing		
	mobile devices		
	mobile phone/smartphone		
	laptop/netbook/notebook		
	tablet		
	handheld game console and other entertainment devices		
	smartwatches and fitness trackers		
	digital cameras		
	virtual reality and augmented reality sets		
	fixed, networked devices with processing and/or storage		
	server		
	Personal Computer (PC)/workstation		
	printer		
	scanner		
	Network Attached Storage (NAS)		
	multi-functional devices (any combination of devices in B2.1.1)		
	connectivity devices		
	switch, managed and unmanaged		
	router, wired and wireless		
	gateway		
	bridge		
	repeater		
	access point		
	USB hub, active and passive		
	modem		
	Digital Subscriber Line (DSL)/copper cable		
	optical fibre modem		
	wireless modem		
	multi-functional devices (any combination of devices in B2.1.2)		
	connection media		
	cable		
	Ethernet		
	universal serial bus (USB), current types and legacy requirements		
	Wireless		
	Wi-Fi, IEEE 802.11 family of standards		
	NFC		
	Bluetooth, current types and legacy requirements		
	cellular, 5G		
	optical fibre		
	Li-Fi		
	Application and security issues of external media and storage		
	encryption		
	secure disposal		

		loss/theft of media		
		interception/copying		
		data loss/corruption		
		media lifespan/failure		
		malware vector		
		Application and features of software components		
		network and device operating systems		
		Graphical User Interface (GUI)		
		Command Line Interface (CLI)		
		web interface, internal web page for device control/configuration		
		network monitoring, management and troubleshooting tools		
		remote access administration tools		
		performance monitor		
		events and logs viewer		
		vulnerability scanner		
		network analyser/packet sniffer		
		network applications		
		remote working tools		
		database		
		document management		
		network discovery/mapping tools.		

B3 Networking infrastructure services and resources

Content			Revised	
	Application and function of:			
		Transmission Control Protocol/Internet Protocol (TCP/IP)		
		four layer model		
		Transport Layer Security (TLS)		
		packets and headers		
		error correction		
		ports		
		hardware, switch ports		
		software/virtual, Internet Protocol ports		
		packet		
		header		
		trailer/footer		
		payload/body/content		
		types		
		- Transmission Control Protocol (TCP)		
		- Internet Protocol (IP)		
		- User Datagram Protocol (UDP)		
		network address translation (NAT)		
		types		
		- static		
		- dynamic		
		- Port Address Translation (PAT)		
		structure and format of IPv4 and IPv6 addressing		
		RFC 1918 private addresses		
		- Class A: 10.0. 0.0 to 10.255. 255.255		
		- Class B: 172.16. 0.0 to 172.31. 255.255		
		- Class C: 192.168. 0.0 to 192.168. 255.255		
		- Automatic Private IP Addressing (APIPA) for DHCP failure, 169.254.0.1to 169.254.254.255		
		- reserved IP addresses such as 127.0.0.1 loopback address		
		Application of domains, sub-domains and segmentation		
		hierarchy		
		trust relationships		
		access control		
		security benefits		
		limits access to devices, data, and applications		
		restricts lateral movement of attack/malware/intruder		
		smaller attack surface		
		simpler damage control		
	Application of network devices to configure networks			
		server		

	router		
	switch		
	Wireless Access Point (WAP)		
	firewall		
	bridge		
	gateway		
Application and function of network infrastructure services			
	Domain Name System (DNS)		
	DNS resolution process		
	reverse DNS resolution		
	DNS cache		
	IPv6 DNS		
	directory services (DS), identity and access management		
	active directory		
	open directory		
	OpenLDAP		
	authentication services		
	types		
	- single-factor		
	- two-factor (TFA)		
	- multi-factor (MFA)		
	- single sign on (SSO)		
	authentication protocols		
	- Password Authentication Protocol (PAP), (RFC 1334)		
	- Challenge Handshake Authentication Protocol (CHAP), (RFC 1994)		
	- Extensible Authentication Protocol (EAP), (RFC 5247)		
	Dynamic Host Configuration Protocol (DHCP)		
	DHCP servers and clients		
	IP address allocation process		
	basic configuration settings		
	- address ranges		
	- lease information		
	- reservations/static addresses		
	- dynamic addresses/allocation		
	- automatic addresses/allocation		
	- server address		
	routing		
	static		
	dynamic/adaptive		
	routing tables		
	Interior Gateway Protocols (IGPs), within one network/organisation		
	Exterior Gateway Protocols (EGPs), between networks		
	Border Gateway Protocol (BGP), internet routing		
	remote access services		
	by dial-up, using telecommunications services		
	by VPN, over the internet		

		• handshake/connection processes, client-host/server		
		• uses/gives access to		
		○ devices		
		○ files		
		○ data		
		○ desktops		
		○ applications		
		Application and function of network services and resources		
		file and print services		
		• file server, networked file storage		
		• print server, networked printer		
		• file management, tracking, sharing		
		• print management, sharing, queueing, prioritising		
		• printer configuration and driver management		
		web, mail and communications services		
		• web services		
		○ use HTTP or HTTPS protocols		
		○ use XML messaging system		
		○ are independent of operating system or programming language		
		○ allow applications to communicate		
		○ allow sharing of data, functionality		
		• mail services		
		○ use Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), and Multipurpose Internet Mail Extensions (MIME)		
		○ protocols lack built-in encryption		
		○ mail server and client		
		○ process of finding destination server for mail delivery		
		○ communications services		
		○ email		
		○ Voice over IP (VoIP)/Internet Calling		
		○ SMS/text Messaging		
		○ video conferencing		
		○ social networking applications		
		○ online collaboration tools		
		○ Communication as a Service (CaaS)		

Name:

BTEC IT Extended Certificate – Unit 2 Content and Revision List



C) Cyber security documentation

Students should know and understand the governance policies and documents needed to establish and maintain security on an ongoing basis.

C1 Internal policies			
Content			Revised
	Use of general security-related IT policies and their effectiveness		
	a cyber security policy that uses the Plan-Do-Check-Act loop derived from part of the International Organization for Standardization (ISO) 27001:2013		
	• policies on internet and email use		
	○ inappropriate, offensive, illegal material		
	○ sending confidential information		
	○ privacy issues		
	○ upload/download of copyrighted material, music, video		
	○ download of executable files		
	○ visiting potentially dangerous websites		
	○ organisations rights and obligations to scan traffic, monitor activities, retain copies of emails, etc.		
	• security and password procedures		
	○ length/strength policy		
	○ management and enforcement tools		
	○ deny lists of common/weak passwords		
	○ monitoring/logging of password attempts		
	○ lockout policy for inactivity, login attempts		
	○ use of technology to reduce requirement for passwords		
	• staff responsibilities		
	○ complete required security training		
	○ follow security procedures and report problems		
	○ respond to/report suspicious activity		
	○ maintain security in own workspace/behaviour		
	• staff IT security training		
	○ leadership/management to ensure training is staffed/funded/resourced		
	○ flexibility of training program so everyone can take part		
	○ range of training resources/learning styles		
	○ progress tracking		
	○ incentives rather than punishment		
	○ ongoing training for reinforcement and for new threats		
	• security audits and their application to check compliance against policies		
	○ audit goals and scope		
	○ identify problems/gaps/weaknesses		
	○ check against internal policies		
	○ check against external regulations/laws		
	○ reporting of results, required improvements/changes		
	backup policy		

		• selection of data		
		• backup methods		
		• backup type		
		• frequency/scheduling		
		• storage strategy		
		• responsibility, accountability		
		• backup testing strategy		
		• legal/regulatory compliance		
		• emergency/recovery procedures		
		data protection policy to ensure organisational compliance		
		• Data Protection Officer		
		• follow data protection principles		
		• protecting rights/privacy		
		• staff training		
		• system security procedures		
		• application of policy to external contractors/consultants/vendors etc.		
		• responsibility and accountability of staff/organisation		
		cyber security incident response policy		
		• contacts		
		○ incident response team leader/provider		
		○ IT team leader/provider		
		○ senior management		
		○ legal		
		○ public relations		
		○ human resources		
		○ insurance		
		• procedures/flowcharts/checklists for		
		○ initial decisions/triage/escalation		
		○ main response, analysis, containment, mitigation, recovery		
		○ reviewing, reporting, closing the incident		
		communications		
		○ contact telephone plus alternative/backup		
		○ conference call facility		
		disaster recovery policy		
		• purpose and scope		
		• triage, a list of possible events, their severity and appropriate response		
		○ activate cyber security incident response		
		○ activate business continuity plan		
		○ activate disaster recovery plan		
		• roles, responsibilities		
		• contact lists		
		• monitoring and reporting requirements		
		external services policy		
		• general for external services policies		
		○ authorization and access control		
		○ management, responsibility, accountability		
		○ contact details		
		○ regulatory compliance		
		○ incident response procedures		

		• cloud		
		○ cloud resources requiring protection		
		○ acceptable use		
		○ data protection		
		• hardware		
		○ sources, vendors, contractors, other third parties		
		○ service agreements		
		○ maintenance and support		
		• software		
		○ sources, vendors, contractors, other third parties		
		○ service agreements		
		○ licencing		
		○ software support		
		• support		
		○ service time/availability		
		○ response time – report to support starting		
		○ troubleshooting/completion/solution time, time to fix the problem		
		○ escalation procedures		

D) Forensic procedures

D1 Forensic collection of evidence

Students should apply their knowledge and understanding of the methods for collecting forensic evidence following a security incident

Content		Revised	
	Forensics on devices – servers, PCs and mobile devices		
	meeting requirements for forensics		
	confiscation of devices		
	- prior planning for a range of devices/scenarios		
	- passwords, codes, PINs, etc		
	- chargers, cables etc. for mobile devices		
	- retain current power state/status if possible		
	- isolation of device from network/communications (if device is suspected to be communicating)		
	- photograph screen		
	- turn off device		
	- remove battery/power cable		
	- use airplane mode		
	- disable wireless communication		
	- use Faraday bag/cage		
	- appropriate packaging		
	- document chain of custody		
	- establish legal permissions		
	- taking an image of the system		
	- using a forensic analysis tool		
	- reviewing files and settings		
	- reviewing system logs		
	- reviewing user activity		
	- malware analysis and alerts		
	the challenges of live forensics		
	changing data in situ		
	recovering corrupted data and preventing data corruption		
	capturing data in active memory		
	capturing remote data		
	not losing temporary files		
	network forensics		
	agreeing a network-testing forensics methodology with supervisory and investigatory authorities		
	scanning of local infrastructure		
	- ensuring permission is granted		
	- ensuring that testing protocol will not disrupt a live system		
	- passive and active analysis tools		
	reviewing and analysing firewalls and infrastructure devices		
	- switch		
	- router		

		○ Wireless Access Point (WAP)		
		○ client or server logs		
		• analysing malware activity and alerts		
		Documenting the scene		
		• prior planning for a range of scenarios		
		• securing the scene		
		• plans, photos, diagrams of the scene		
		• contemporaneous notes		
		• witness statements		

D2 Systematic forensic analysis of a suspect system

Students should apply their knowledge and understanding of the requirements and processes for forensic analysis

Content	Revised	
Requirements for maintaining an accurate record, made at the time, or as soon after the incident as possible		
Retaining snapshots of the system		
originals/clean system for comparison		
generate hash function/checksum for copies/images		
whole disk/machine, with/without 'boot' facility		
files/folders directories/data structures		
memory, RAM, BIOS, memory cards/SIM		
virtual discs/machines		
process/sub-process output/activity		
network information such as open ports, IP addresses, user logins		
temporary files, deleted data		
system generated data such as System Volume Information, hibernation files, shadow copies, crash dumps, page files, synchronisation files		
Requirements for the recording of all findings and considering how reliable the evidence is		
no collection/action that could change data on a digital device		
collection by competent person		
creation of trail or record of all actions taken, chain of custody		
documentation of who is responsible for collection/decisions/enforcement of standards		
Requirements for the recording of any alterations that have been intentionally and unintentionally imposed by the investigator		
documentation of all actions from initial seizure		
potential inadmissibility of altered data		
working with copies/images rather than original data/device		
Requirements for the creation of visual evidence of findings		
photos, videos		
screenshots		
data-time stamps. metadata		
Ensuring the evidence is relevant and not a false positive		
defining file signatures, search criteria, etc.		
known/estimated error rates of tools/target data types		
feedback of false positive data to improve detection method/algorithm		
alert fatigue for high false positive rates		
manual review of all positives to filter obvious false ones		
further investigation/check of filtered positives		
Assessing the findings to determine whether or not they:		
provide evidence of a crime and/or an incident		
criminal		
regulatory breach		
civil liability, contractual breach		

		• non-compliance with internal policy		
		• cyber attack		
		• negligence, mismanagement, etc		
		show that the system has been externally and/or internally compromised		
		• unusual traffic		
		○ inbound		
		○ outbound		
		○ from unusual geographical regions		
		○ DoS/DDoS signs		
		• unusual login attempts		
		• unusual login attempts		
		• unusual DNS requests		
		• increase in file/data reads		
		• increase in file/data requests		
		• unusual port usage		
		• suspicious changes to files/data		
		• suspicious access to/changes to system files/data		
		Writing security reports on		
		actions to prevent security incidents from reoccurring in the future		
		• general report structure		
		○ title		
		○ contents		
		○ introduction		
		○ headings and sub-headings		
		○ consistent use of bullets and numbering		
		○ conclusions		
		○ footnotes		
		○ citations		
		• analysis of the incident to identify		
		○ errors/omissions in procedures		
		○ unforeseen problems		
		○ errors/omissions in preventative measures		
		○ errors/ delays in detection/alerting		
		○ remedial actions		
		improvements to the content of IT policies		
		improvements to security protection measures		
		• physical		
		• software		
		• hardware		
		• processes and procedures		
		• training		