CYBER SECURITY TECHNICAL PROFESSIONAL INTEGRATED DEGREE APPRENTICESHIP STANDARD

Role Profile: A cyber security technical professional operates in business or technology / engineering functions across a range of sectors of the economy including critical national infrastructure (such as energy, transport, water, finance), public and private, large and small. They will normally operate with a considerable degree of autonomy and will lead teams which research, analyse, model, assess and manage cyber security risks; design, develop, justify, manage and operate secure solutions; and detect and respond to incidents. They work in accordance with applicable laws, regulations, standards and ethics.

Typical Job Roles: Cyber Risk Manager; Cyber Risk Analyst; Cyber Research Analyst; Cyber Incident Manager; Cyber Security Engineer; Cyber Security Design Engineer.

Entry Requirements: individual employers will set the selection criteria, but this is likely to include three 'A' levels, including maths, or other relevant qualifications or experience.

A cyber security technical professional has the competencies, knowledge and underpinning skills attitudes and behaviours below.

Technical Competencies	Technical Knowledge and Understanding
1: N/A	Foundations of cyber security, its significance, concepts, threats, vulnerabilities and assurance.
2: Design, build, configure, optimise, test and troubleshoot simple and complex networks.	Network foundations, connections, internetworking, protocols, standards, performance, security and server virtualisation.
3: Apply statistical techniques to large data sets. Identify vulnerabilities in big data architectures and deployment.	Information management, big data concepts, statistical techniques, database concepts and data quality.
4: Build test and debug a digital system to a specification.	Computer architecture, digital logic, machine level representation of data.
5: Configure an Operating System in accordance with security policy. Identify threats and features.	Operating System principles, architectures, features, mechanisms, security features and exploits.
6: Write, test, debug programs in high and low level languages and scripts.	Algorithm and program design, concepts, compilers and logic. Programming languages.
7: Design, implement and analyse algorithms.	Algorithms, complexity and discrete maths.
8: Construct software to interact with the real world and analyse for security exploits.	How software interacts with the hardware and real world environment and security issues.
9: Analyse malware & identify its mechanisms.	Malware, reverse engineering, obfuscation.
10: Apply secure programming principles and design patterns to address security issues.	Defensive programming, malware resistance, code analysis, formal methods, good practice.
11: Apply system engineering and software development methodologies and models.	System development principles, tools, approaches, complexity, software engineering.
12: Discover, identify and analyse threats, attack techniques, vulnerabilities and mitigations.	Threats, vulnerabilities, impacts and mitigations in ICT systems and the enterprise environment.
13: Assess culture & individual responsibilities.	Human dimensions of cyber security.
14: Undertake ethical system reconnaissance and intelligence analysis.	Structured and ethical intelligence analysis, methods, techniques.
15: Undertake risk modelling, analysis and trades.	Management of cyber security risk, tools and techniques.
16: Undertake risk assessment to an external standard.	Quantitative & qualitative risk management theory & practice, role of risk stakeholders.
17: Apply a management system and develop an information security management plan.	Concepts & benefits of security management systems, governance & international standards.
18: Configure and use security technology components and key management.	Security components: how they are used for security / business benefit. Crypto & key

	management.
19: Design & evaluate a system to a security case.	How to compose a justified security case.
20: Architect, analyse & justify a secure system.	Understand security assurance, how to achieve it and how to apply security principles
21: Develop an assurance strategy.	Assurance concepts & approaches.
22: Security monitoring, analysis and intrusion detection. Recognise anomalies & behaviours.	How to diagnose cause from observables. Application of SIEM (Security Information and Event Management) tools & techniques.
23: Manage intrusion response, including with 3rd parties.	Cyber incident response, management, escalation, investigation & 3rd party involvement.
24: N/A	Legal, regulatory, compliance & standards environment.
25: Organise testing & investigation work in accordance with legal & ethical requirements.	Applicability of laws regulations & ethical standards.
26: Develop & apply information security policy to implement legal or regulatory requirements.	Legal responsibilities of system owners, users, employers, employees.

Underpinning professional, interpersonal and business skills

- Fluent in written communications and able to articulate complex issues.
- Makes concise, engaging and well-structured verbal presentations, arguments and explanations.
- Able to deal with different, competing interests within and outside the organisation with excellent negotiation skills.
- Able to identify the preferences, motivations, strengths and limitations of other people and apply these insights to work more effectively with and to motivate others.
- Able to work effectively with others to achieve a common goal.
- Competent in active listening and in leading, influencing and persuading others.
- Able to give and receive feedback constructively and incorporate it into his/her own development and life-long learning.
- Analytical and critical thinking skills for Technology Solutions development and can systematically analyse and apply structured problem solving techniques to complex systems and situations.
- Able to put forward, demonstrate value and gain commitment to a moderately complex technology-oriented solution, demonstrating understanding of business need, using open questions and summarising skills and basic negotiating skills.
- Can conduct effective research, using literature and other media.
- Logical thinking and creative approach to problem solving.
- Able to demonstrate a ‘security mind-set’ (how to break as well as make).

Behaviours

- Demonstrates business disciplines, ethics and courtesies, demonstrating timeliness and focus when faced with distractions and the ability to complete tasks to a deadline with high quality.
- Flexible attitude and ability to perform under pressure.
- A thorough approach to work in the cyber security role.

Qualifications: BSC (Hons) Cyber Security Technical Professional Degree. Apprentices without Level 2 English and maths must achieve this prior to taking the end-point assessment.

Professional Recognition: recognised for entry to Institute of Information Security Professionals membership at Associate level.

Duration: the duration of this apprenticeship is typically 48 months.

Level: this is a Level 6 apprenticeship.

Review Date: this standard will be reviewed three years from the publication date.