| Role Profile | ICT Technical Security Lead | Devon & Cornwall POLICE |
|---|---|---|

## Section 1 – Job Description

Principal responsibilities, duties and activities required of the postholder. To be used for measuring performance.

The principal responsibility of the ICT Technical Security Lead is to lead the ICT Security area providing technical security services and protective monitoring services to the Alliance. With responsibilities that include but are not limited to:

- Establishing, maintaining and monitoring, in conjunction with other Alliance personnel and third parties, appropriate service level, availability, configuration, capacity, change and release management processes for ICT security services
- Assess all changes to ICT systems, applications, processes and services for security implications and advise accordingly. With an emphasis on securely enabling business needs rather than blocking them.
- Providing accurate and detailed advice and guidance to the Alliance in the feasibility and impact of strategic and tactical changes to the ICT security, systems and services
- Lead teams – in-house, third party and partner - in the development and installation of appropriate ICT security solutions, often within the context of an agreed project methodology, so as to support the delivery of improved operational performance or to offer other clear business benefits
- Leading the team tasked with the day to day support of the Alliance ICT services, ensuring that they perform to agreed Force standards and service levels and within budgetary constraints
- Provide feedback to staff on performance, support development of them and their teams and undertake line management responsibilities
- Running ICT security protective monitoring services with other Alliance personnel, 3rd parties and others
- Managing the Alliance's ICT security "defence in depth" through management of equipment and processes of firewalls, patching, end-point, anti-virus (etc.)
- Prepare for and manage security incidents and any recovery activity that results, with others in ICT, Alliance and 3rd parties
- Prime point of contact and key liaison with Alliance Information Assurance function
- Lead within ICT for ICT Service Continuity Management, owning processes associated with Service and Business continuity manager. Authoring the ICT "Bronze" and "Silver" business continuity plans for the Alliance ICT Department
- Working with Operations/Contingency Planning, Corporate Communications (web team) suppliers and government bodies to promote ICT service continuity and cyber-resilience
- Maintain engagement and acting as a core member of the Computer Emergency Response Team (CERT) process
- Maintain engagement and acting as a key ICT liaison point into Operational / Business Continuity Department

| **Department** | Alliance ICT |
|---|---|

## Section 2 – Terms of Role

Corporate terms of the role, including pay banding, restrictions and pre-requisites required for appointment.

| | | | | | |
|---|---|---|---|---|---|
| **Resource Type** | Police Staff | **Grade** | GR8 | **SCP Range** | 36 - 40 |
| **Vetting Clearance** | SC | **Position Code** | P4713 | **JE Ref.** | C270 |
| **Political Restrictions** | N/A | **Biometrics (DNA / Fingerprints)** | | | N/A |

| **Medical Assessment** | N/A |
|---|---|
| **Role-Specific Training to be undertaken** | |
| • Leadership and Management CPD<br>• ITIL Service Practitioner qualification – where not held, to achieve within 2 years of appointment<br>• Project management qualification (Prince2 or Agile)<br>• CISMP (Certificate in Information Security Management Principles) – where not held, to achieve within first year of appointment<br>• CISSP (Certified Information Systems Security Professional) – where not held, to achieve within 2 years of appointment<br>• Business Continuity qualification - where not held, to achieve within 2 years of appointment | |

| **Section 3 – Special Conditions & Additional Information** | |
|---|---|
| ℹ | Additional or special conditions required of the postholder. |
| **1** | Successful completion of the Police Staff Induction and mandatory Health & Safety e-learning packages. |
| **2** | Where not already held, the qualifications/certifications specified in 'Role Specific Training' should be achieved during appointment in the time frames. If not achieved, where there are no exceptional circumstances, relevant performance procedures will commence. |

| **Section 4 – Essential Criteria** | |
|---|---|
| ℹ | Essential qualifications, experience, knowledge and skills required for this role. To be used for recruitment and selection purposes. |
| **1** | Business Continuity qualification, or achieve in post |
| **2** | Significant experience in the configuration and administration of ICT security solutions and services |
| **3** | Experience of working with 3rd party suppliers in the delivery of end to end ICT services |
| **4** | Understanding of the range of services available through ICT security protective monitoring services |
| **5** | Experience in managing complex "defence in depth" and "recovery activities" for ICT security |
| **6** | Demonstrable understanding of business and service continuity links to ICT security |
| **7** | In Depth understanding of IT security matters including design, implementation and monitoring skills relating to Firewall, Operating Systems and Networks |
| **8** | Knowledge of encryption system design, implementation and monitoring |
| **9** | Experience of leading (e.g. Cisco, Microsoft) Operating System Architectures and use of ICT monitoring tools and processes |
| **10** | Familiar with the ITIL best practices and procedures |
| **11** | ICT project management experience. Familiar with the project life cycle in an IT environment. |
| **12** | Effective Communication Skills. Able to communicate with Operational and Business levels of the Alliance through meetings, presentations and written reports. A willingness to share knowledge and provide quality documentation to colleagues |
| **13** | Proven ability to evaluate and quantify new security threats and accreditation standards against existing and future business requirements |
| **14** | Understanding of ICT security and background understanding of legal issues relating to ICT |
| **15** | Experience of managing people and activities delivering mission-critical technical security services within large organisations |
| **16** | Proven ability to analyse and use information methodically to identify problems and draw logical conclusions |
| **Competency Value Framework (CVF) Level** | **Level 2** |

| | |
|---|---|
| ℹ | Under each competency are three levels that show what behaviours will look like in practice. This role has been identified as the above CVF level. See the Competency Value Framework (CVF) guidance provided alongside this role profile, to view the behaviours for the associated CVF level. |

| **Competencies** |
|---|
| We are emotionally aware |
| We take ownership |
| We collaborate |
| We support and inspire |
| We analyse critically |
| We are innovative and open-minded |

| **Section 5 – Version** | |
|---|---|
| ℹ | No changes should be made to this role profile without HR approval. Please contact Grading & Pay for changes or amendments relating to this role profile. |
| **Version Date** | 06/07/2026 |