Job Title:	**Information Assurance Officer**
Reporting to:	Chief Information Security Officer
Date:	May 2019
Location	Flexible – Remote working, Prolinx Offices and Customer Sites.

Brief overview of the role:	The security of information is critical to the ongoing success and reputation of the business. The role of Information Assurance (IA) Specialist will offer the successful candidate an exciting opportunity to work closely with the business across a broad range of activities (projects, new product developments, business processes, stakeholder advice and strategy) to ensure that information is used in a secure and appropriate manner. This role will ensure that compliance and accreditation commitments are achieved and completed for the secure hosted solutions that are provided by the business. The role of IA Specialist will also form part of the core security team that deliver and drives continual service improvement across the business ensuring delivery of best of breed compliant security services in the most effective and efficient manner. The role requires the successful candidate to undergo and achieve high levels of security clearance to fulfil the job role.
Duties:	Main Duties of the Job: The IA Specialist will report directly to the Chief Information Security Officer and will work with other internal teams as well as customer points of contact in order to ensure IA requirements are met. Day to Day the role will include creating, reviewing and updating security documentation required by our customer base in order to enable the usage of secure solutions that Prolinx provide. Below are some key responsibilities: • Identify security risks within complex classified systems and ensure adherence to MoD policy and standards. • Engage with stakeholders to ensure that risk to the confidentiality, integrity and availability of data is documented and managed pragmatically, appropriately and in a cost effective manner. • Understand technical designs and controls to ensure appropriate risk levels are established. • Develop and maintain RMADS in accordance with MoD Standards and policy. • Register Systems and applications onto necessary registration systems.

	• Discuss and explain security risks and controls to customers, internal teams and stakeholders.
Essential Skills and Experience	The following skills and experience would be ideal, however training can be provided to achieve these standards if required. • Experience on defence/central government IT systems. • Knowledge and understanding of MoD, UK Government Standards, Policies, Guidance and Legislation. • Knowledge of Accreditation life-cycle of a System. • Experience of IT risk assessments, risk management and accreditation document sets. • Knowledge of IT technical topics such as backups, anti-virus, patching, password policies and group policy settings etc. • Experience of IT risk assessment documentation and understanding of how to control/mitigate IT risks. • Demonstrable understanding of security risks within complex systems and ability to address risks through controls and mitigation. • Excellent communication skills and the ability to provide stakeholders with an appropriate level of technical information. • Risk Management in the UK Defence Sector. • Experience in writing RMADS, RBC's and other MOD documents. • Experience with DART, DAR and DIMP.
Personal Attributes	The following personal attributes would be desirable: • Interest in IT Security and an understanding of a Security Incident. • Analytical & Problem solving skills • Excellent Time Management & organisational skills • Good communication skills and demonstrable leadership skills • Ability to work autonomously or as part of a Team • Proficient in the use of MS Office Applications. • A passionate and committed professional who strives to achieve company goals and is self-motivated to work from any location. • An extremely high level of self-integrity and discretion at all times.

Equal Opportunities

Prolinx does not discriminate on the basis of race, religion, colour, sex, age, disability or sexual orientation. All recruitment decisions are based solely on qualifications, skills, knowledge and experience and relevant business requirements.

The Job Holder will understand the regulatory, fair trading and competition rules relating to their work sufficiently to be able to comply with them, relying on their knowledge or on their ability to recognise that they will need specialist support.

The Job Holder will actively support at all times company policy and best practice in the area of security, with particular emphasis on the protection of sensitive customer information. This includes the Security requirements of our customers