JOB DESCRIPTION & PERSON SPECIFICATION

Job Title: Cybersecurity Lead	**Location:** Hunmanby / Mansfield
Department: Engineering	**Contract:** Permanent
Reports To: Technical Director	**Direct Reports:** None

1.0 Job Summary & Role

Deep Sea Electronics Ltd (DSE) are a leading UK electronics manufacture specialising in development of advanced control and automation products for the power generation and off highway vehicle markets. Our range of solutions include connected devices that are subject to the latest cybersecurity standards.

The cybersecurity lead will be responsible for overseeing cyber security aspects our products. They will work closely with cross functional teams including engineering, operations and commercial to ensure products regulatory compliance and industry best practices.

2.0 Key Responsibilities & Main Duties

- Lead the cybersecurity program at DSE Ltd
- Coordinate, develop and maintain the cybersecurity strategy and policies for development of products within DSE product range
- Work cross functionally with other departments to ensure full coverage of the relevant cyber security regulations, including the EU Cyber Resiliency Act.
- Work with product management to drive cyber security initiatives into the product road map
- Lead the identification, assessment, and mitigation of cybersecurity risks associated with product development and deployment
- Oversee the preparation and submission of necessary documentation for compliance with IEC 62443 and related regulatory requirements
- Ensure continuous alignment with industry regulations and frameworks related to industrial cybersecurity
- Collaborate with engineering teams to integrate security features into product design and architecture
- Advise on secure software development practices and secure by design principles
- Lead vulnerability assessments, threat modelling, and penetration testing efforts for product solutions

- Ensure secure remote access, network security, and secure communication protocols are implemented throughout the products
- Act as the primary point of contact for cybersecurity incidents and response within the product development lifecycle
- Work with internal teams to implement lessons learned from security incidents and continuously improve security measures
- Conduct post-incident reviews and develop preventative measures to mitigate future risks
- Serve as a cybersecurity subject matter expert for internal and external stakeholders
- Educate and train internal teams on cybersecurity best practices, emerging threats, and mitigation strategies
- Work closely with customers and regulatory bodies to address cybersecurity requirements and concerns

3.0 Internal & External Relationships

- Engineering Management team – assist with the implementation of cyber security projects
- Test and Approvals department – assist with training and in the development of test programs and procedures for cyber security
- Technical Support – assist technical support with more involved customer queries, and technical authoring support including review of security manuals
- Commercial sales team – Support customer faces sales literature and promotion of cyber security awareness at DSE

4.0 Key Performance Indicators

- Attention to detail, able to work both individually as a part of a team and self-discipline required for software developing and testing
- Produce clear and concise software documentation
- High quality software development
- Ability to define and work to timescales

5.0 Essential/Desirable Factors

Knowledge	
Essential: - Expert in C/C++ for embedded systems - Cyber security development processes, including risk assessment techniques - Security protocols and techniques, encryption, key storage, secure boot and trust zones. - Knowledge of RED and CRA regulations	**Desirable:** - Embedded Linux operating systems - IoT systems - Electrical principles - Functional safety experience, alongside cyber security

- Cyber security standards, IEC 62443, EN18031	
Skills & Attributes	
Essential: - Familiar with stage gated / agile development approaches - Comfortable collaborating and communicating with embedded systems engineers and company executives alike, bridging the gap between technical and management - Ability to lead a team through cyber risk analysis, pragmatically - Use to work to working to high levels of quality and accuracy standards - Ability to translate requirements into a technical product specification - Used to work in a high-pace environment - Enthusiastic and optimistic	**Desirable:**
Experience	
Essential: - Held a role focused on cyber security in embedded systems - Worked practice of the relevant standards - Leadership of primary contributor to risk analysis, mitigations and translation requirements	**Desirable:** - Industrial protocols such as RS485, CAN - Background in industrial control and automation products
Qualifications	
Essential: - BSC in computer science or related degree qualification	**Desirable:**

Created by	**Dated Created**
Scott Preece	21/03/2025