

JOB DESCRIPTION



Section 1: General information	
Job title:	Cyber Security Analyst
Department:	IT
Reports to:	Head of IT
Version:	1
Section 2: PenCarrie's story and What we are looking for	
PenCarrie's story: With 30 years' experience, PenCarrie has built a strong reputation as a leading B2B supplier to the garment decoration industry. Based in Willand, Devon, PenCarrie stocks over 4,000 product lines, 80,000 SKU's from over 80 of the industry's top brands from promotional t-shirts to high specification outdoor wear. With a primary focus on meeting the needs of customers, PenCarrie delivers not just on choice but on customer service, reliability and the values that make it one of the leading companies in the market. We are a family business employing around 300 Team PenCarrie Members, each of whom is as passionate about the business as the next. What we are looking for: The distribution partner that enables exceptional customer success.	
Section 3: Responsibilities of the role	
Main purpose of role: The Cyber Security Analyst is responsible for protecting PenCarrie's information assets, systems, infrastructure and cloud services by maintaining and continually improving PenCarrie's cyber security posture. The role is responsible for monitoring security systems, responding to security incidents, identifying and managing vulnerabilities, supporting compliance activities and ensuring security is considered throughout the delivery of IT services and projects. Working collaboratively across the business, the Cyber Security Analyst builds strong and respectful relationships with colleagues and third-party partners, actively looks for ways to help the business succeed, embraces change and continually strives to improve PenCarrie's security posture, helping create a secure environment. Main responsibilities: 1. Support the design, implementation and continual improvement of PenCarrie's cyber security architecture across infrastructure, cloud services and business applications. 2. Develop, review and maintain IT security policies, standards, procedures and technical baselines that are clear, transparent and aligned with business needs. 3. Support the maintenance, testing and continual improvement of the Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). 4. Maintain an up-to-date understanding of the cyber security landscape, emerging threats, vulnerabilities and security technologies, recommending improvements where appropriate. 5. Administer, monitor and optimise enterprise cyber security technologies including endpoint protection, identity and access management, cloud security, vulnerability management, data protection, security awareness and network security platforms. 6. Monitor security alerts, investigate suspicious activity, lead technical investigations and coordinate responses to cyber security incidents. 7. Perform vulnerability assessments, coordinate remediation activities, validate security fixes and report on vulnerability trends. 8. Conduct regular security reviews, audits and configuration assessments to ensure systems remain secure and aligned with recognised best practice.	

9. Support compliance activities including Cyber Essentials Plus, PCI DSS, GDPR and other applicable regulatory or business requirements.
10. Support the Legal team with data protection and information security matters, providing clear and transparent technical advice for GDPR compliance, data breaches, security incidents and risk assessments.
11. Support the implementation, administration and continual improvement of Data Loss Prevention (DLP), information protection and data classification technologies.
12. Support the implementation, operation and continual improvement of Security Information and Event Management (SIEM), Security Operations Centre (SOC) and Extended Detection and Response (XDR) capabilities.
13. Produce security reports, dashboards and metrics, providing recommendations to reduce risk and improve PenCarrie's overall security posture.
14. Support the secure implementation of new infrastructure, applications and cloud services by ensuring security requirements are considered throughout project delivery.
15. Build strong and respectful relationships with internal teams and third-party suppliers to investigate security issues, manage risks and deliver security improvements.
16. Develop and deliver engaging cyber security awareness initiatives, helping colleagues understand cyber risks, make informed decisions and create a safe and inclusive workplace where everyone can thrive.
17. Review threat intelligence, security advisories and vendor notifications, assessing potential impact and coordinating appropriate remediation activities.
18. Support the secure adoption of Artificial Intelligence technologies by promoting appropriate governance, risk management and compliance with company AI policies.
19. Participate in an out of hours support rota and provide technical support during Major Incidents and cyber security incidents where required.
20. Continually review PenCarrie's security posture, looking forward, anticipating emerging threats and striving to improve PenCarrie's cyber resilience through innovation and continual improvement.

Section 4: Person specification

Knowledge, skills and experience required:

Essential

- Administration of Microsoft 365 and Microsoft Azure security technologies.
- Enterprise endpoint protection, identity and access management, cloud security and information protection technologies.
- Vulnerability management platforms and vulnerability remediation processes.
- Delivery of cyber security awareness training and phishing simulation programmes using platforms such as KnowBe4 or equivalent.
- Understanding of networking concepts, firewalls, VPNs and secure network design.
- Understanding of cyber security principles, threat detection, incident response and security monitoring.
- Knowledge of Data Loss Prevention (DLP), information protection and data classification principles.
- Awareness of Security Information and Event Management (SIEM), Security Operations Centre (SOC) and Extended Detection and Response (XDR) concepts.
- Excellent written, verbal and interpersonal communication skills.
- Strong analytical and problem-solving skills.

JOB DESCRIPTION



- Production of technical documentation, reports and procedures.
- Sound judgement and confidence to make informed technical decisions.
- Strong organisational skills with the ability to prioritise competing workloads.
- Collaborative approach, building strong and respectful relationships with colleagues, suppliers and stakeholders.
- Clear and transparent communication, with the ability to explain technical security concepts to both technical and non-technical audiences.
- Commitment to continual improvement, embracing change and proactively identifying opportunities to strengthen PenCarrie's cyber security posture.
- Self-motivated, proactive and able to work independently while contributing positively to team objectives and helping create a safe and inclusive working environment.
- Flexibility to work outside normal working hours when required.

Desirable

- Experience with Microsoft Sentinel or other SIEM platforms.
- Experience with Microsoft Defender XDR.
- Experience with Fortinet firewalls.
- Experience with Data Loss Prevention (DLP) and Microsoft Purview Information Protection.
- Experience working with Security Operations Centre (SOC) or Managed Detection and Response (MDR) services.
- Experience supporting Cyber Essentials Plus, PCI DSS, GDPR or ISO 27001.
- Experience with PowerShell scripting or automation.
- Relevant cyber security certifications (CompTIA Security+, Microsoft Security, SC-200, SC-300, SC-900, CISSP, CISM or similar).
- Degree in a relevant IT or Cyber Security discipline.

Section 5: Key Contacts

Internal: Head of IT, IT team, Executive Committee, Heads of Departments, Legal, People & Culture and colleagues across all business departments.

External: IT suppliers, software and security vendors, managed service providers, external auditors, cyber security consultants and other third-party partners.

PenCarrie Values

We're dedicated to customer success

- Every one of us can make a difference to our customers' experience
- We actively look for ways to help our customers succeed
- Our customers are considered in every decision we make

We build strong and respectful relationships

- We create a kind, safe and inclusive workplace where everyone feels they can thrive
- We collaborate to find solutions and build ideas
- We build trust in each other
- We're prepared to have the difficult conversations, giving and receiving feedback

We look forward and embrace change

JOB DESCRIPTION



- We're bold, brave and inspirational
- We look up, look out and look forward
- We anticipate and embrace change

We're proud of everything we do

- We strive to improve in everything we do
- We celebrate our achievements
- We all have a voice
- We know our priorities and implement with conviction and pace



We grow responsibly

- We use our resources wisely
- We're clear and transparent in our communications to all our stakeholders
- We're committed to reducing our environmental impact
- We give back to our communities

Section 5: Job description prepared by

Job title: Head of IT

Date: June 2026