JOB DESCRIPTION

Section 1: General information	
Job title:	IT Security Analyst
Department:	IT
Reports to:	Head of IT

Section 2: PenCarrie's story and purpose

PenCarrie's story:

With over 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 3,500 product lines from over 75 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 300 Team PenCarrie members each of whom is as passionate about the business as the next.

PenCarrie's purpose:

The distribution partner that enables exceptional customer success.

Section 3: Purpose and responsibilities of the role

Main purpose of role:

The IT Security Analyst performs two core functions for PenCarrie. The first is the day-to-day operations of the in-place security solutions while the second is the identification, investigation and resolution of security breaches detected by those systems. Secondary tasks may include involvement in the implementation of new security solutions, participation in the creation and or maintenance of policies, standards, baselines, guidelines and procedures as well as conducting vulnerability audits and assessments. The IT Security Analyst is expected to be fully aware of PenCarrie's security goals as established by its stated policies, procedures and guidelines and to actively work towards upholding those goals.

Main responsibilities:

1. Planning and design of security architecture under the direction of the IT leadership, where appropriate.
2. Creation of security documents (policies, standards, baselines, guidelines and procedures) under the direction of the IT leadership, where appropriate.
3. Planning and design of a Business Continuity Plan and Disaster Recovery Plan, under the direction of the IT leadership, where appropriate.
4. Maintain up-to-date detailed knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.
5. Recommend additional security solutions or enhancements to existing security solutions to improve overall security.
6. Perform the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and the security documents specifically.
7. Ensure up-to-date baselines for secure configuration and operations of all in-place devices including security tools, workstations, servers and network devices.
8. Maintain operational configurations of all in-place security solutions as per the established baselines.
9. Monitor all in-place security solutions for efficient and appropriate operations.
10. Analyse logs and reports from all in-place devices, interpret implications of detected activity and devise actionable plans for resolution.
11. Lead investigations into suspicious or problematic activity, ensuring thorough analysis and resolution.
12. Design and conduct vulnerability assessments, penetration tests, and security audits to identify and address potential security risks.
13. Provide on-call support for end users for all in-place security solutions.

JOB DESCRIPTION

Section 4: Person specification

Knowledge, skills and experience required:

Essential
- Virtualisation platform experience (VMware preferred)
- Understanding of network hardware and technologies
- Microsoft cloud service, Azure/Microsoft 365, including familiarity with security tools i.e. Azure Security Centre or Microsoft Defender
- Windows Operating Systems
- Wireless network configuration
- Excellent written and spoken communication skills, interpersonal and analytical skills
- Technical documentation/reporting
- Ability to make decisions on technically complex issues
- Flexibility to work outside of normal working hours throughout the year as well as in different locations

Desirable
- Firewall configuration experience
- Microsoft Group Policy
- IP Telephony system experience
- Linux or Mac OS Operating Systems
- Degree in a relevant field
- Relevant IT qualifications

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
- 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: October 2024