ALLPAY LIMITED

Job Description

Owner	HR Manager	**Date Created**	28/01/2010 14:48:00
Classification Level	Public	**Template Version**	General Form v1.4

1. JOB IDENTIFICATION

Job Title: **Cyber Security Specialist**

Responsible to: **Cyber Security Lead**

Department(s): **IT**

2. JOB PURPOSE

This is a pivotal role in the day to day operational security of the entire IT department, and therefore the security of allpay.

Reporting to the Cyber Security Lead, the post-holder will be instrumental in maintaining a pre-emptive and pro-active security alert status within the IT department, both to keep systems and services secure from threats, and to ensure systems and services comply with regulatory requirements and controls through log analysis, scanning, assesments and investigation.

Working with the IT team and broader business to ensure that new products, changes, older systems and technologies are integrated / configured and secured in line with IT security and compliance principles, policies and best practice set by the likes of PCIDSS and ISO27001.

This role will play a pivitol part in Incident and Problem Management ensuring compliance with the IT Security policy and best practices

3. DIMENSIONS

You will be part of a new Cyber security team embedded within the IT function. You will be responsible for ensuring that all work being completed across the various disciplines in IT are assessed in terms of vulnerabilities and exposure to internal or external attack.

You will be responsible for managing various operational systems that monitor and assess allpay's cyber security posture. This may include incidents generated by a SIEM, track remediation of vulnerabilities detected in applications and infrastructure, and external Pen tests.

As part of your role, you will be expected to support the Technical Design Authority group who will vet any new project work intending on being completed (including small changes) in both hardware or software terms. The TDA will continue to review progress at key milestones throughout project delivery.

Aside from the TDA, the role is expected to act as a 'friendly policeman', assisting the development and infrastructure teams on introducing best practice for hardening our defences. This means that you will work to ensure processes and procedures incorporate all the necessary steps as integral to that of a developer or infrastructure engineers' role.

You will work closely with our colleageues in the compliance team to ensure that areas of non-compliance are addressed.

4. ROLE OF DEPARTMENT

The role of the cyber security team is to be proactively working to uncover and address IT risks, and to make sure that our live systems are resilient from cyber attack, both internally and externally.

The team will be working with infrastructure and software development to review all of the existing systems for vulnerabilities and to make sure processes and procedures are adopted in the allpay IT landscape so that no new systems being built are introducing further risk.

5. KEY RESULT AREAS

Identifying and addressing a full range of issues from structure and policy, through to assisting in specific areas such as data privacy, data leakage prevention/monitoring, information rights management, third party security and cryptography

Network Forensics, Windows Forensics, Mobile Device Forensics, Threat Hunting, Threat Intelligence (Consumption & Production), Malware Analysis (Static & Dynamic) inclusive of reverse engineering in addition to general client-facing/soft-skill abilities.

Support stakeholders with both onsite and remote assurance activities including audits.

Provide expert advice across a range of Cybersecurity risk domains including technical security controls.

Work as part of the Technical design authority to assess cyber security risks in any new applications being built and to advise on where additional work must be put into development or architecture to mitigate against security risks that may occur.

Work with the head of software delivery and the software development manager to design and develop audit strategies (automated and manual) to measure the effectiveness of information security controls for each internally built application.

Perform internal vulnerability monitoring on hardware and software.

Coordinate and build management reports, and scorecards addressing risk and vulnerability

Proactively offer guidance and support to colleagues across the business on Cyber Security and to support and mentor all IT staff on best practices.To highlight security risks within the wider allpay business.

Display pride in own work and the reputation of allpay in the Cyber Security field

Take ownership for work and objectives

Follow through on commitments and support this behaviour across the team and department

Demonstrate resilience under very demanding pressures and circumstances

6. ADDITIONAL KEY DUTIES

You will expected to provide ad-hoc out of hours additional support during a major incident (Severity 1 or 2) where the business need demands it.

In business areas where regular issues will occur, you may be expected to form part of an out of hours rota system.

At the time of a major incident, you may be asked to perform an emergency job role away from your regular role. This will be led and managed by the incident manager at the time of the incident until such a time where the incident is deemed by the incident manager to be over. You will not be expected to do both duties during that time, however, the new role may be significantly different from your regular role.

7. KNOWLEDGE, TRAINING, EXPERIENCE & SKILLS REQUIRED TO DO THE JOB

InfoSec/CyberSec experience is essential.

Experience with ISO27001 and PCI-DDS.Awareness of GDPR, Compliance, Awareness Training, Governance, Security Strategies and Risk Management.

Knowledge and expertise in monitoring systems inc. SIEM & Intrusion Detection

Ability to address multiple assignments simultaneously, with strong ability to prioritize tasks, and respond to dynamic priorities.

Proven track record of working in infrastructure or application security.

A strong attention to detail and excellent writing and analytical skillset.

MS Office and PowerPoint proficient.

Cyber Maturity Assessments.

Penetration and Vulnerability testing experience.

Experience of Security Incident Management.

Demonstable knowledge of Sniffer software.

Knowledge of network devices and firewalls, Web and Email filters, server and workstation operating systems.

Awareness of OWASP and understanding of the OWASP top 10.

Familiarity with working in an ITIL Framework.

Able to learn and stay current with new techniques, attack vectors and vulnerabilities.

Certifications such as:

- CISSP, GSEC, Security+, CPSA, CPIA, or equivalent.

Previous experience working within the Financial Services sector.

8. JOB DESCRIPTION AGREEMENT

We confirm that this conveys a full and accurate description of the job as at	
Job Holder's Name and Signature:	Date:
Manager of Department Name and Signature:	Date:
Director of Department Name and Signature:	Date: