APM-L-4 IT Operations Security Analyst

Information Services (IS)

Reporting to: IT Operations Team Leader

Job Family and level: APM Level 4

Contract Status: Permanent

Hours of Work: Full time

Location: Kings Meadow Campus

You are a technical specialist in one or more infrastructure and/or networking technologies deployed at the University. You will play a key role contributing towards the on-going support, maintenance, design, development and management of core University IT services. You possess strong organisational skills and have excellent attention to detail. You are a proficient communicator, who is at ease dealing with staff at all levels, and are confident in building relationships across organisational boundaries. You are delivery and customer focussed and will take a hands-on approach to help secure success as we respond to the constantly evolving IT landscape.

The University

The University of Nottingham (UoN) is ranked in the UK's top 10 and the world's top 75 universities by the Shanghai Jiao Tong (SJTU) and the QS World University Rankings, placing it in the top 1% of all universities worldwide. UoN has award-winning campuses in the UK, China and Malaysia and is committed to providing a truly inspiring and international education. Described by The Sunday Times University Guide 2011 as 'the embodiment of the modern international university' – the University of Nottingham is uniquely enterprising and renowned for its production of world-leading research.

Information Services

Many of our services are typical of any business and offer similar challenges: Managed desktops and laptops, data storage, email, printing, web content management for the internet and intranet, data and voice networking, multimedia design and production, and the major applications underpinning finance, HR/payroll, marketing, facilities management, conferencing and a range of commercial enterprises, including incubator premises for new business ventures.

Other challenges are specific to higher education and to our University in particular. Nottingham has huge ambition to transform the experience it provides to students — to place them at the heart of its global, digital community. This will involve fundamental change to the business processes which underpin the student journey through the institution, major organisational change across professional services teams, and the implementation of a comprehensive, integrated suite of supporting IT systems. We, in Information Services, will play a pivotal role in this exciting and challenging change programme — known as Transform.

We also run specialist systems to underpin the life cycle of each research project as it moves from grant application through to publication and dissemination. Our researchers need information to help them target the next exciting and lucrative research opportunity. They need to be able to demonstrate the impact their research is having in the world.

As our mission says, "by bold innovation and excellence in all that we do, we make both knowledge and discoveries matter". This depends on getting the right information to the right people within our community. Here, the creation, sharing, analysis and dissemination of information are defining activities. It’s what we exist to do. Both students and researchers are demanding, innovative users of technology and we aim to provide them an information environment in which they can be boundlessly creative and highly productive. We have campuses in Nottingham, China and Malaysia, and aim to support mobility, ease of communication and team work across this hugely diverse and geographically spread community.

In response to these specific challenges, we provide particular and differentiating services. These include a Virtual Learning Environment and other innovative technologies for learning, High Performance Computing services and a large range of specialist software. Our researchers produce vast amounts of data and need tools to manage, mine and generate information from it. Many of them collaborate with industrial partners and researchers in other institutions across disciplinary and organisational boundaries. Our students have grown up with internet technologies and expect to be constantly connected using their mobile devices. A technology-rich experience is what they expect from University life. We provide equipment in teaching rooms, PC suites, language laboratories, wireless everywhere, and internet services in the halls of residence. Our global nature also means that video conferencing is particularly important.

Context

Following the appointment of a new CIO, Information Services (IS) is undergoing a significant restructuring and reinvigoration. The aim is to build an organisation which can be the reliable, trusted, innovative and agile IT partner that the University needs to deliver its ambitious 2020 Strategy across the UK, China and Malaysia campuses. Part of the change is to develop project delivery capability, an architecture capability and a service delivery capability that work together to deliver the right solutions at the right time and cost and ensure that the solutions are properly and predictably understood, used, managed and supported and replaced.

IT Operations; we express the purpose of Infrastructure Technology Operations as: “To keep the IT infrastructure running well, available and secure.”

IT Operations is part of Global Service Delivery. It is responsible for all the daily operations, preventative maintenance, reactive support and upgrades necessary to manage and protect the IT Infrastructure and major business applications. It safeguards the stability of the entire production environment across the Data Centres and a distributed network spanning all of the University campuses. Where applications are externally hosted, it is responsible for the daily management of the appropriate external supplier. Team members also play key roles in projects which will upgrade, enhance or otherwise impact services (i.e. all projects), ensuring that all systems are designed to be manageable, secure, robust and supportable, and can be smoothly transitioned into Operations.

Your Role

The Security Analyst will be responsible for monitoring all computer systems connected to the university network to identify known vulnerabilities, potential weaknesses, unusual activity and unauthorised or illegal activity.

The role holder will have responsibility for providing support for the University’s centrally managed anti-virus solution, assisting with the installation and testing of software and security updates for the Windows Operating Systems, regular Endpoint performance monitoring, tracking, analysis, optimisation, and usage reporting.

In collaboration with the Security & Endpoint Group Leader, you will assist in the production of information security best practice and document the current acceptable secure computing practices. This role will also involve project participation where security and Endpoint management is a consideration.

The role holder will be expected to work closely with the service management team to ensure consistent reporting and feedback of security related incidents and problems.

	Main Responsibilities	**% time per year**
	1. Monitor all computer systems connected to the university network: • Identify known vulnerabilities, compromised systems and unauthorised activity • Implement security updates and provide 3rd line support for issues affecting the vulnerability of systems and services • Monitor usage and performance of existing security services to react quickly and decisively to any new security threats or diagnose problems • Ensure accurate documentation, recording and reporting to ensure quality information provision (e.g. SupportWorks, security reports, inventory, monthly group reports) • Support the security assessment process such as penetration testing, vulnerability analysis, audits and anomaly detection • Maintain security solutions to enable consistent function and support of a range of operating systems and applications across the University	50%
	Analyse and champion security solutions across the University: • Provide support for the automatic distribution systems for installing, securing and updating a range of operating systems and applications • Respond to security incidents to identify the method of attack used, determine the damage caused and recommend any action required to prevent reoccurrence. • Provide detailed information and documentation to 1st line support teams to ensure effective and efficient troubleshooting activity (e.g. Knowledgebase, Process maps) • Involvement in security incident activities with other groups such as IT support teams, data centre team, the network team, the police and JANET Computer Security Incident Response Team • Support automatic distribution systems for installing, securing and updating of a range of operating systems and application software • Consult with other IT staff, departmental system administrators and end users to advise on how best to secure network servers and personal workstations	20%
	Platform Ownership • Perform the role of Platform owner for one or more platforms as defined in appendix A	20%
	Other	10%

	• Promote secure computing practices through seminars and published documents • Assist other team/group members and provide technical support cover for other platforms when required • Ensure currency of knowledge and skills by tracking relevant developments through meetings and contact with hardware and software suppliers and peers within the industry and academia, to enable the university to benefit from cost effective innovative solutions consistent with IS strategy • Participation in the out of hours on-call service, to protect the University's computing services in the event of systems outages and incidents • Provide support and mentoring to other less experienced team members	

Knowledge, Skills, Qualifications & Experience

	Essential	**Desirable**
Qualifications/ Education	• Degree or equivalent in IT-related subject or equivalent relevant experience	• ITIL Service Management certificate • Industry relevant and recognised IT security certification
Skills/Training	• Competent skill set; • A good working knowledge of a range of a range of desktop and Server Operating Systems in particular Windows and Linux / Unix and all associated aspects of administration, patch management, installation and support. • Good understanding of Anti-Virus and Anti-Spyware solutions, and the mechanisms required to prevent and respond to virus outbreaks • Has over 2 years' recent experience in current versions. • Familiar with networking services and able to specify connectivity requirements and diagnose connectivity problems • Excellent analytical and problem solving skills • Good all round knowledge of infrastructure technologies supported by other teams within Information Services • Ability to work in a team, to deadlines and under pressure and also to work effectively with minimal support, for example, outside working hours	• Knowledge Apple based desktop solutions • Understanding of enterprise email systems (eg Exim).

	• Ability to communicate effectively within a large organisation and to build a network of contacts • Awareness of current IT legislation and best practice in relation to Information Security and an ability to apply them in practice • Excellent communication, analysis and problem-solving skills • Proven ability to prioritise and schedule workloads in the face of conflicting demands • The ability to rapidly assimilate and deploy detailed technical knowledge in specialist areas • Willingness to travel from site to site within Nottingham and the UK. • Excellent customer/supplier facing skills; Confident presenter, with influencing and negotiation skills • Willingness to take responsibility for Platform and Services in a global context	
Experience	• Track record of contributing to large scale security focused projects • Strong experience administering a range of desktop and server operating systems • Involvement working with external suppliers • Experience of administering and configuring of Endpoint security solutions • Significant experience of supporting automated solutions for enterprise wide Anti-virus and security patch distribution • Familiarity with username and directory administration • Familiar with networking services and able to specify connectivity requirements and diagnose connectivity problems • Experience in the support, maintenance and configuration of the relevant infrastructure technologies • Experience of working within a structured IT Service Delivery Framework • Experience of delivering IT services in a complex and large-scale environment • Experience of using Service Desk tools and applications within an ITIL environment	• Knowledge of the Higher Education environment • Experience of transformational IT change programs • Practical experience of designing and implementing solutions for a large distributed organisation

Additional Information

Due to the nature of the Team’s remit, flexibility and a broad range of skills, knowledge and expertise are key to responding to the wide variety of problems and incidents that unpredictably occur during the day to day work of the Team. Although the role holder will be based at the Kings Meadow Campus, they will be required to work at other Campus’ as required. The University of Nottingham is a global 24hour operation and therefore in order to minimise the impact on the University’s day-to-day operations it may be necessary for the role holder, on occasions, to undertake some IT Operational activities outside of the standard working day and at weekends.

Behavioural Competences

Serving the Customer

This is the desire to anticipate, meet and exceed the needs and expectations of customers (internally and externally). It implies working together, building long-term customer relationships and focusing one's efforts on delivering increased customer value. At levels 4 and 5 it requires effective championing and partnership working;

- Acts as customer champion
- Make systems/ procedures more customer-friendly and challenges University to provide them;
- Tries to get other colleagues across the University to see things from the customers' perspective - acts as a customer champion;
- Develops an understanding of customer needs in order to anticipate service needed

Quality Focus

This is about demonstrating the underlying drive to ensure that quality is not compromised within the working environment. It includes the identification and maintenance of standards to meet the needs of the University, together with a desire for accuracy, order and safety in the workplace. At levels 4 it is about encouraging and monitoring the actions of others to maintain high standards;

- Monitors the standards of others
- Sets up appropriate quality review processes;
- Audits the work of others to ensure that procedures are being followed;
- Seeks feedback from customers and colleagues to ensure quality standards are being maintained;
- Uses a range of techniques to keep projects or activities on track;
- Monitors the progress of work against project milestones and/or agreed standards of work;
- Where development needs are highlighted, arranges appropriate interventions;
- Seeks to define and communicate quality standards

Problem Solving and Initiative

This is about engaging in proactive behaviour, seizing opportunities and originating action which goes beyond simply responding to the obvious needs of the situation or to direct requests from others. It is coming up with new or different ideas, or adapting ideas from elsewhere in the University or externally. It is concerned with moving the University forward by applying new ideas or old ideas in a new way to generate solutions and approaches. At the higher levels it is about thinking laterally and creating new concepts;

- Generates a range of innovative ideas
- Is open minded and actively seeks opportunities to try out new ideas;
- Takes action in areas for which he/she has no direct personal responsibility;
- Have a record of seizing and driving ideas and opportunities to successful implementation;
- Produces novel ideas to modify procedure and performance;
- Tries to break new ground and be creative when generating solutions;
- Creates innovative working methods to generate new ideas;
- Uses resources creatively and thinks laterally to identify new solutions;
- Has a flexible approach to problem solving;
- Looks beyond the obvious and immediate information when generating solutions;
- Demonstrates resourcefulness in identifying and exploiting trends and developments

Communicating with Clarity

This is about the ability to impart accurate information (both verbal and written) in a timely way and be receptive to other peoples' opinions. It is also about sharing information across University boundaries and externally. At the higher level, it is about making University communication and understanding with other bodies outside the University more effective;

- Focuses on improving University-wide communications
- Sets up processes to improve information flow at a wider University level;
- Actively promotes and provides information across the University to avoid duplication of effort and encourage cross team working;
- Engages in sharing and seeking to develop mutual understanding between different constituencies both within and outside the University;
- Communicates persuasively when required.

Collaborating with Others

This competency implies the intention of working co-operatively with others, to be part of a team, to work together as opposed to working separately or competitively. For this behaviour to be effective, the intention should be genuine. Team work and co-operation may be considered whenever the subject is a member of a group of people functioning as a team. This competency emphasises activity as a member of a group (rather than as a leader); e.g. reflects a peer supporting their group rather than a leader managing the group;

- Encourages others
- Openly praises other members of the team when they have done something well and gives credit for good team work;
- identifies and works to the strengths of team members;
- Identifies what motivates different individuals and uses this knowledge to improve performance;
- Empowers other members of the team, making them feel strong and important;
- Encourages colleagues after a set back

Planning, Organising and Flexibility

This is about adopting a methodical approach to work. It involves planning and organising oneself and others in order to deliver work and prevent future problems. This includes the ability to adapt and change plans as the requirements of the situation change. At the higher levels it involves thinking long-term, strategically and creatively;

- Plans ahead and adapts
- Involves others in planning activities;
- Shifts resources to ensure delivery;
- Monitors and manages staff skills and competence to ensure sufficient resources are available to meet expectations;
- Assesses time and resources needed for projects or activities;
- Develops practical and realistic plans that ensure efficient use of resources;
- Plans how to deal with peaks and troughs in workload over time;
- Draws up contingencies and adapts plans as necessary

Critical Information Seeking

Critical information seeking requires a selective approach to gathering information aimed at getting the really crucial pieces of information. The ability to seek out information based on an underlying curiosity or desire to know more about subject area, University issues, people, and the sector. It includes asking questions that go beyond what is routine, in order to 'dig' or press for exact information. Critical information seeking is essential for making sure your decisions are firmly grounded in reality, and that they are the best they can be;

- Digs deeper
- Gets important information that others wouldn't get;

- Contacts others who are not personally involved to get their perspective or benefit from their experience;
- Is well known as an active listener;
- Gathers information from all key ‘stakeholders’ (i.e. people with vested interests);
- Allows others to discuss to identify issues;
- Finds out in detail how fellow colleagues have tackled a particular problem;
- Asks a series of probing questions to get to the root of a situation or problem; doesn't stop with the first answer, but finds out the underlying reasons why something has happened;
- Builds knowledge of how the University works and the factors which impact on business performance;
- Makes sure that 'no stones are left unturned' when investigating an issue

Drive for Results

Success is not just about following the rules. We need people committed to making the University a success. ‘Drive for results’ is the enthusiasm and desire to meet and exceed objectives, University targets and improve one’s own performance. It is about being frustrated with the status quo, wanting to improve the way we do things and making it happen. At a higher level it is about calculated risk taking in the interest of improving overall University performance;

- Generates a range of innovative ideas
- Is open minded and actively seeks opportunities to try out new ideas;
- Takes action in areas for which he/she has no direct personal responsibility;
- Have a record of seizing and driving ideas and opportunities to successful implementation;
- Produces novel ideas to modify procedure and performance;
- Tries to break new ground and be creative when generating solutions;
- Creates innovative working methods to generate new ideas;
- Uses resources creatively and thinks laterally to identify new solutions;
- Has a flexible approach to problem solving;
- Looks beyond the obvious and immediate information when generating solutions;
- Demonstrates resourcefulness in identifying and exploiting trends and developments

Embracing Change

This is about the ability to make changes to the way you work, adapting to changing circumstances in the University by accepting new and different ideas and approaches. It includes the ability to sustain performance under conditions of rapid change. At higher levels, it is concerned with supporting others through change and having the willingness and ability to enable changes to take place in the most productive way;

- Enables and shapes change
- Creates a sense of shared vision and excitement for change;
- Helps others see the University and personal benefits of the change;
- Creates processes and practices which facilitate the implementation of change;
- Paces change appropriately for others; balancing needs for speed of change with needs of the University and individual

Innovation and Creativity

This is about creating and identifying novel approaches to address challenging academic, technical or commercial situations and problems. It is about coming up with new or different ideas, or adapting ideas from elsewhere in the University or externally. It is concerned with moving the University forward by applying new ideas or old ideas in a new way to generate solutions and approaches. At the higher levels it is about thinking laterally and creating new concepts;

- Identifies and tries out different approaches
- Modifies an existing idea to produce something that can be applied personally;

- Tries out a number of different solutions;
- Speeds up and improves existing processes by using a different approach;
- Applies learned models and theories to current business situations;
- Is open minded and actively seeks opportunities to try out new ideas and situations;
- Generates alternatives before settling on a solution;
- Develops new approaches to improve or replace existing procedures or systems

Appendix A Platform Owner Role

To be Responsible and primary point of contact for the Platform with the Accountability residing with the Infrastructure Service Manager or the appropriate Service Manager

To work with IT Service Management to define and agree 'The Service' and associated Service Levels and Key performance Indicators (KPI) reporting.

To agree and deliver, to the required frequency, a data set for reporting purposes which allows the Service Manager to compile the relevant service related reports.

To ensure support and management of the platform is maintained in accordance with the defined quality targets (KPI) and adheres to the relevant Operational Level Agreements (OLA) or Service Level Agreements (SLA).

To discuss, agree, document and present changes to the underlying infrastructure platform with the appropriate interested parties including Technical Assessment Board (TAB) and Change Advisory Board (CAB)

To ensure all changes affecting the Platform are properly assessed for technical merit in accordance with the existing Change Management policy and that Change Control is rigorously applied.

To act as the initial point of contact for the vendors and suppliers that we use to provide assurance for our platform services. Work closely with the Supplier Relationship Managers, Infrastructure Services Manager, Datacentre and Licensing Manager to ensure that all necessary underpinning maintenance/support contracts are in place to support the platform.

To assist in the annual budgeting and quarterly forecasting process providing relevant information in a timely fashion.

To develop an investment plan (including hardware, licences and management tools) for the platform based on known and predicted requirements, budgetary constraints and in alignment with vendor roadmaps. To review these annually with Infrastructure Services Manager and Technical Architect function to ensure that this is in alignment with and supports the Enterprise Architecture's Technology Road Map.

Keep abreast of latest vendor developments (vendor road maps)

To produce relevant Management Information for the platform (capacity trends) in a timely fashion which feeds the capacity planning process and supports the business case for additional investment. Also provide data and information to the relevant Service and Operational Managers which will help drive Continual Service Improvements in both effectiveness and efficiency.

To own issues and problems associated with the platform on behalf of the Operations function. Provide regular updates and inputs into the Weekly Red Amber Green (RAG) report and problem review meetings by monitoring and trending incidents and producing relevant management information reports which could also be used to identify service improvements

To produce and maintain documentation pertaining to the platform ensuring all those involved in the delivery of the platform have appropriate levels of access

Working with the Infrastructure Services Manager produce a Service Continuity plan and associated test plans which must be reviewed, tested and maintained on a regular basis as required. The minimum should be annually.

To take ownership of the actions in the Risk Register arising from resilience reviews, audits and major incidents. Ensure they are updated and progressed in accordance with their priority

To take accountability for the decision making process affecting the Platform and maintain a record of these for auditing purposes

Working with Service and Operational Management define, agree and communicate appropriate use policies relevant to the platform ensuring alignment with existing policies (E.g. Code of Practice for use of University computer facilities)

In conjunction with Line Management identify the key technical personnel responsible for the delivery of the platform and under pinning services and ensure they maintain the required level of skills to support it