Resources for Chapter 8 – Roles and competencies

RESOURCES

- **Job description template - Information Security Manager**
- **Job description template - Senior Information Security Specialist**
- **Job description template - Information Security Specialist**
- **SFIA competencies**
- **Collaboration between security administrators and academic researchers – UCL, case study**

Job description template - Information Security Manager

Job grade Management and Specialist Grade

Job purpose

- Provides leadership and guidelines on information assurance security expertise for the organisation, working effectively with strategic organisational functions such as legal experts and technical support to provide authoritative advice and guidance on the requirements for security controls.
- Provides for restoration of information systems by ensuring that protection, detection, and reaction capabilities are incorporated.
- Develops strategies for ensuring both the physical and electronic security of automated systems.
- Ensures that the policy and standards for security are fit for purpose, current and are correctly implemented.
- Reviews new business proposals and provides specialist advice on security issues and implications.

Duties and responsibilities

- Develops information security policy, standards and guidelines appropriate to business, technology and legal requirements and in accordance with best professional and industry practice.
- Prepares and maintains a business strategy and plan for information security work which addresses the evolving business risk and information control requirements, and is consistent with relevant IT and business plans, budgets, strategies, etc.
- Operates as a focus for IT security expertise for the organisation, providing authoritative advice and guidance on the application and operation of all types of security control, including legislative or regulatory requirements such as data protection and software copyright law.
- Manages the work of all other IT security specialist staff, including project and task definition and prioritisation, quality management and budgetary control, and management tasks such as recruitment and training when required.
- Manages the operation of appropriate security controls as a production service to business system users.
- Develops implementation approach, taking account of current best practice, legislation and regulation. Ensures implementation of information security strategy in automated systems and ensures operations of security systems. Analyses results of investigations into complex, or highly sensitive security violations, to determine whether standards are fit for purpose, are current and are correctly implemented.
- Reports any significant breaches in security to senior management. Interviews offenders in conjunction with the relevant line manager or on own authority if the breach warrants it. Where appropriate, participates in forensic evidence gathering, disciplinary measures, and criminal investigations.
- Ensures that procedures are in place for investigation of system access enquiries referred by support staff and for handling all enquiries relating to information security, contingency planning as they affect the activities of the organisation, function or department. Authorises implementation of procedures to satisfy new access requirements, or provide effective interfaces between users and service providers.
- Devises new or revised procedures relating to security control of all IT environments, systems, products or services in order to demonstrate continual improvement in control including creation of auditable records, user documentation and security awareness literature.
- Authorises and initiates the provision of training, guidance and support to other security administrators and their agents within the employing organisation, in all aspects of security policy and control.
- Reviews new business proposals and planned technical changes and provides specialist guidance on security issues and implications.
- Maintains knowledge of the technical specialism at the highest level.
- Keeps in close touch with and contributes to current developments in the technical specialism within employing organisation, own industry and in appropriate professional and trade bodies. Is fluent at articulating best practice and is a recognised authority in the technical specialism.
- Be familiar with relevant University IT-related procedures and policies (acceptable use, data protection, freedom of information, information security, purchasing etc) and advise colleagues and end-users accordingly.
- Undertake various other tasks on an occasional basis at the request of more senior staff in the department, and to a level commensurate with training, knowledge, grade and skills.

Note: This job description was created in the spirit of the BCS (The Chartered Institute for IT), SFIA (Skills for the Information Age) level 6 with support from the BCS.

Organisational Responsibility

Responsible to: <line manager> but may receive strategic instruction from the Director of IT.

Responsible for: A team of <x> colleagues, staff at the senior level may be asked to deputise for their line manager in case of absence.

Hours: 37 hours per week, within the hours of 8:00 to 18:00 Mon to Thursday and 8:00 to 17:30 Friday, including 1 hour lunch period. The precise pattern of working within these guidelines will be agreed in advance with your manager.

Special Conditions

Many staff carry mobile phones which allow them to be paged by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills, and takes account of the personal commitments and wishes of individuals.

For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must at all times respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or his/her nominee.

Please note: <organisation> is working towards equal opportunities and observance of our equal opportunities policy will be required.

PERSON SPECIFICATION

Job Title: Information Security Manager

Job Grade: Management and Specialist Grade

Department: IT Services

All staff have a statutory responsibility to take reasonable care of themselves, others and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

	Essential	Desirable	Stage to be assessed
Experience	Demonstrates extensive knowledge of good security practice covering the physical and logical aspects of information products, systems integrity and confidentiality		Shortlisting
		Experience in managing a customer facing service.	Shortlisting
	Demonstrates strong examples of the use of: Principles, practices, tools and techniques of IT auditing.		Interview
		Experience within the HE/FE sector.	Shortlisting
	Displays a responsible attitude to following procedures, keeping records, and caring for equipment and other assets.		Shortlisting & Interview
	Demonstrated success in deploying methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.		Shortlisting & Interview

	Essential	Desirable	Stage to be assessed
Skills and abilities	Shows aptitude for analysing and managing problems arising from incidents in the operation of information systems, combined with the ability to provide innovative technical solutions		Shortlisting & Interview
		Technical background in multiple modern Operating Systems (Windows, Mac OS X, Linux etc)	Shortlisting
	High levels of technical investigation skills, the ability to research and collate information from a variety of sources into technical reports and recommendations.		Shortlisting
		Expert skills in the application of forensic techniques.	Shortlisting
	Demonstrates excellent communication skills with an aptitude for dealing with users, colleagues and suppliers.		Interview
		Technical authoring experience and proven documentation track record.	Shortlisting & Interview
	Familiar with Methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.		Shortlisting & Interview
	Excellent written skills to write technical procedures, reports, system specifications etc.		Shortlisting
	Excellent time management		Shortlisting
	Ability to schedule your own workload and prioritise your work.		Interview
Training and Education/ Qualifications	A willingness to undertake further training and to learn and adopt new procedures as and when required.		Interview
	Ability to assimilate technical information and keep up-to-date in your field.		Shortlisting & Interview
	Degree with relevant IT/Computing content OR relevant professional IT qualifications and/or experience.		Shortlisting
		Information Security related qualifications: CISSP, CISM or similar	Shortlisting
		ITIL Foundation training and accreditation.	Shortlisting
		Formal management training	Shortlisting
Other	To observe the organisation's Equal Opportunities policy at all times.		Interview

Stages in assessment: **Shortlisting, Test (where appropriate) and Interview**

Conditions of Service

The appointment will be on a **full time, open ended** contract on **Management and Specialist Grade (salary, discretionary to salary per annum)*** at a starting salary commensurate with experience and qualifications.

*The appointment will be subject to the University's normal Terms and Conditions of Employment for **Academic and Related** staff, details of which can be found at:

<Terms and Conditions Link>

Informal Enquiries

Informal enquiries should be made to **<name>**, **<title>** by email at: <email address> or by telephone on **<telephone number>**.

Application

The closing date for receipt of applications is **<insert>**.

Job description template - Senior Information Security Specialist

Job grade Management and Specialist Grade

Job purpose

- Obtains and acts on vulnerability information and conducts security risk assessments for business applications and computer installations; provides authoritative advice and guidance on security strategies to manage the identified risk.
- Investigates major breaches of security, and recommends appropriate control improvements. Interprets security policy and contributes to development of standards and guidelines that comply with this.
- Performs risk assessment, business impact analysis and accreditation for all major information systems within the organisation.
- Ensures proportionate response to vulnerability information, including appropriate use of forensics.
- Drafts and maintains the policy, standards, procedures and documentation for security.
- Monitors the application and compliance of security operations procedures and reviews information systems for actual or potential breaches in security.
- Ensures that all identified breaches in security are promptly and thoroughly investigated.
- Ensures that any system changes required to maintain security are implemented. Ensures that security records are accurate and complete.

Duties and responsibilities

- Conducts security control reviews across a full range of control types and techniques, for business applications and computer installations. Seeks guidance from more experienced or specialised practitioners as required. Recommends appropriate action to management.
- Identifies threats to the confidentiality, integrity, availability, accountability and relevant compliance of information systems. Conducts risk and vulnerability assessments of business applications and computer installations in the light of these threats and recommends appropriate action to management.
- Conducts investigation, analysis and review following breaches of security controls, and manages security incidents. Prepares recommendations for appropriate control improvements, involving other professionals as required.
- Provides authoritative advice and guidance on the application and operation of all types of security controls, including legislative or regulatory requirements such as data protection and software copyright law. Contributes to development of standards and guidelines.
- Drafts and maintains policy, standards, procedures and documentation for security administration, taking account of current best practice, legislation and regulation. Ensures that all identified breaches in security are promptly and thoroughly investigated. Interviews offenders in conjunction with the relevant line manager or on own authority if the breach warrants it.
- Reviews information systems for actual or potential breaches in security, and investigates complex, or highly sensitive violations referred by more junior staff or colleagues, handling issues imaginatively, efficiently and professionally. Obtains factual information, and formulates opinions regarding exposed violations, through interview with all levels of staff. At all times, undertakes to bring to the attention of management any actual or potential breaches in security.
- Investigates system access enquiries referred by support staff and all enquiries relating to information security, contingency planning, as they affect the activities of the organisation, function or department. Implements and adopts known techniques to satisfy new access requirements, or provides an effective interface between users and service providers when existing facilities are considered inadequate.
- Recognises requirements for, and creates, auditable records, user documentation and security awareness literature for all services and systems within IT Security Management, ensuring that the records provide a comprehensive history of violations, resolutions and corrective action.
- In consultation with senior security personnel, devises and documents new or revised procedures relating to security control of all IT environments, systems, products or services (including physical security) in order to demonstrate continual improvement in control. Ensures that any system changes required to maintain security are implemented.
- Advises on, and assists with the assessment of the potential impact on existing access security mechanisms of specific planned technical changes, in order to help ensure that potential compromise or weakening of existing security controls is minimised. Also assists in the evaluation, testing and implementation of such changes.
- Drive liaison with customers and stakeholders in order to pursue continual service improvement and produce customer-driven and well-supported services.
- Delivers and contributes to the design and development of specialist IT security education and training to IT and system user

management and staff.

- Manages the operation of appropriate security controls as a production service to business system users.
- Monitors the application and compliance of security operations procedures, and reports on non-compliance.
- Ensures that training, guidance and support is provided to other security administrators, in all aspects of security policy and control.
- Plans and manages the work of small teams of security staff on complex IT security specialism projects.
- Maintains knowledge of the technical specialism at the highest level.
- Keeps in close touch with and contributes to current developments in the technical specialism within employing organisation, own industry and in appropriate professional and trade bodies. Is fluent at articulating best practice and is a recognised authority in the technical specialism.
- Be familiar with relevant University IT-related procedures and policies (acceptable use, data protection, freedom of information, information security, purchasing etc) and advise colleagues and end-users accordingly.
- Undertake various other tasks on an occasional basis at the request of more senior staff in the department, and to a level commensurate with training, knowledge, grade and skills.

Note: This job description was created in the spirit of the BCS (The Chartered Institute for IT), SFIA (Skills for the Information Age) level 5 with support from the BCS.

Organisational Responsibility

Responsible to: <line manager> but may receive strategic instruction from the Director of IT.

Responsible for: None, staff at the senior level may be asked to deputise for their line manager in case of absence.

Hours: **37 hours per week, within the hours of 8:00 to 18:00 Mon to Thursday and 8:00 to 17:30 Friday, including 1 hour lunch period. The precise pattern of working within these guidelines will be agreed in advance with your manager.**

Special Conditions

Many staff carry mobile phones which allow them to be paged by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills, and takes account of the personal commitments and wishes of individuals.

For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must at all times respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or his/her nominee.

Please note: <organisation> is working towards equal opportunities and observance of our equal opportunities policy will be required.

PERSON SPECIFICATION

Job Title: Senior Information Security Specialist

Job Grade: Management and Specialist Grade

Department: IT Services

- All staff have a statutory responsibility to take reasonable care of themselves, others and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

	Essential	Desirable	Stage to be assessed
Experience	Demonstrated experience in methods and techniques for risk management, business impact analysis, countermeasures and contingency arrangements.		Shortlisting
		Experience of Penetration Testing	Shortlisting
	Demonstrates examples of the use of: Principles, practices, tools and techniques of IT auditing.		Interview
		Experience within the HE/FE sector.	Shortlisting
	Experience of software development and code review		Shortlisting & Interview
	Demonstrated success in deploying methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.		Shortlisting & Interview
Skills and abilities	Shows aptitude for analysing and managing problems arising from incidents in the operation of information systems, combined with the ability to provide innovative technical solutions.		Shortlisting & Interview
		Technical background in multiple modern Operating Systems (Windows, Mac OS X, Linux etc)	Shortlisting
	High levels of technical investigation skills, the ability to research and collate information from a variety of sources into technical reports and recommendations.		Shortlisting
		Expert skills in the application of forensic techniques.	Shortlisting
	Demonstrates above average communication skills with an aptitude for dealing with users, colleagues and suppliers.		Interview
		Technical authoring experience and proven documentation track record.	Shortlisting & Interview
	Familiar with Methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.		Shortlisting & Interview
	Excellent written skills to write technical procedures, reports, system specifications etc.		Shortlisting
	Excellent time management		Shortlisting
	Ability to schedule your own workload and prioritise your work.		Interview
Training and Education/ Qualifications	A willingness to undertake further training and to learn and adopt new procedures as and when required.		Interview
	Ability to assimilate technical information and keep up-to-date in your field.		Shortlisting & Interview
	Degree with relevant IT/Computing content OR relevant professional IT qualifications and/or experience.		Shortlisting
		Information Security related qualifications: CISSP, CISM or similar	Shortlisting
		ITIL Foundation training and accreditation.	Shortlisting
Other	To observe the organisation's Equal Opportunities policy at all times.		Interview

Stages in assessment: Shortlisting, Test (where appropriate) and Interview

Conditions of Service

The appointment will be on a full time, open ended contract on Management and Specialist Grade (salary, discretionary to salary per annum) at a starting salary commensurate with experience and qualifications.*

*The appointment will be subject to the University's normal Terms and Conditions of Employment for Academic and Related staff, details of which can be found at:

<Terms and Conditions Link>

Informal Enquiries

Informal enquiries should be made to <name>, <title> by email at: <email address> or by telephone on <telephone number>.

Application

The closing date for receipt of applications is <insert>.

Job description template - Information Security Specialist

Job grade Management and Specialist Grade

Job purpose

- Investigates identified security breaches in accordance with established procedures and recommends any required actions.
- Assists users in defining their access rights and privileges, and administers logical access controls and security systems. Maintains security records and documentation
- Conducts security risk and vulnerability assessments for defined business applications or IT installations in defined areas, and provides advice and guidance on the application and operation of elementary physical, procedural and technical security controls (e.g. the key controls defined in ISO/IEC 27001).
- Performs risk and vulnerability assessments, and business impact analysis for medium size information systems. Investigates suspected attacks and manages security incidents.

Duties and responsibilities

- Conducts security control reviews in well-defined areas. Assesses security of information and infrastructure components. Investigates and assesses risks of network attacks and recommends remedial action.
- Conducts business risk and vulnerability assessments and business impact analysis for well-defined business applications or IT installations.
- Reviews compliance with information security policies and standards. Assesses configurations and security procedures for adherence to legal and regulatory requirements.
- Reviews network usage. Assesses the implications of any unacceptable usage and breaches of privileges or corporate policy. Recommends appropriate action.
- Provides advice and guidance on the application and operation of elementary security controls (e.g. the key controls defined in ISO/IEC 27001) and communicates information assurance issues effectively to users of systems and networks.
- Supervises and/or administers the operation of appropriate security controls (such as physical or logical access controls), as a production service to business system users.
- Investigates suspected attacks and manages security incidents.
- Maintains awareness of the implication of any legislation or other external regulations, which affect security within any defined scope of activity.
- Investigates and reconciles violation reports and logs generated by automated policing mechanisms in accordance with established procedures and security standards. Investigates any other identified security breaches in accordance with established procedures. Interviews minor offenders and compiles reports and recommendations for management follow-up.
- Assists users in defining their needs for new access rights and privileges. Operates and administers logical access controls and directly associated security services relating to all platforms used in order to provide continuous and secure access to information services.
- For all services and systems within IT Security Management, maintains auditable records and user documentation. Assists in the preparation and maintenance of other documentation such as business recovery plans, particularly in the data collection and compilation/production/distribution phases of the exercise.
- Provides advice and handles enquiries relating to other security, contingency planning and related activities.
- Maintains knowledge of the technical specialism.
- Be familiar with relevant University IT-related procedures and policies (acceptable use, data protection, freedom of information, information security, purchasing etc) and advise colleagues and end-users accordingly.
- Undertake various other tasks on an occasional basis at the request of more senior staff in the department, and to a level commensurate with training, knowledge, grade and skills.

This job description was created in the spirit of the BCS (The Chartered Institute for IT), SFIA (Skills for the Information Age) level 4 with support from the BCS.

Organisational Responsibility

Responsible to: <line manager> but may receive strategic instruction from the Director of IT.

Responsible for: None, staff at the senior level may be asked to deputise for their line manager in case of absence.

Hours: 37 hours per week, within the hours of 8:00 to 18:00 Mon to Thursday and 8:00 to 17:30 Friday, including 1 hour lunch period. The precise pattern of working within these guidelines will be agreed in advance with your manager.

Special Conditions

Many staff carry mobile phones which allow them to be paged by various systems at all reasonable hours of the week. When monitoring, diagnosis and configuration of services needs to be done outside normal working hours, it can sometimes be appropriate for the work to be carried out remotely at home when convenient.

Attendance on site outside normal working hours is occasionally necessary, for example during major system changes and maintenance. Such out-of-hours working as is necessary is scheduled in negotiation with the group of staff with relevant skills, and takes account of the personal commitments and wishes of individuals.

For purposes of system management, IT Services staff often have enhanced access to data, files and computer systems and must at all times respect the privacy of information to which they have enhanced access. The only exception to this will be investigations authorised by IT Services Director or his/her nominee.

Please note: <organisation> is working towards equal opportunities and observance of our equal opportunities policy will be required.

PERSON SPECIFICATION

Job Title: Information Security Specialist

Job Grade: Management and Specialist Grade

Department: IT Services

All staff have a statutory responsibility to take reasonable care of themselves, others and the environment and to prevent harm by their acts or omissions. All staff are therefore required to adhere to the University's Health, Safety and Environmental Policy & Procedures.

	Essential	Desirable	Stage to be assessed
Experience	Familiar with the concepts of risk management, business impact analysis, countermeasures and contingency arrangements.		Shortlisting
		Experience in an Information Security role.	Shortlisting
	Familiar with the use of: Principles, practices, tools and techniques of IT auditing.		Interview
		Experience within the HE/FE sector.	Shortlisting
	Displays a responsible attitude to following procedures, keeping records, and caring for equipment and other assets.		Shortlisting & Interview
	Demonstrated success in the methods, techniques and standards for writing concise and effective reports.		Shortlisting & Interview
Skills and abilities	Shows an analytical and systematic approach to problem solving.		Shortlisting & Interview
		Technical background in at least one modern Operating Systems (Windows, Mac OS X, Linux etc)	Shortlisting
	High levels of technical investigation skills, the ability to research and collate information from a variety of sources into technical reports and recommendations.		Shortlisting
		Awareness of forensic techniques and/or penetration testing.	Shortlisting
	Good communication skills with an aptitude for dealing with users and colleagues.		Interview
		Is familiar with the principles and practices involved in development and maintenance and in service delivery	Shortlisting & Interview
	Familiar with Methods and techniques for preparing and presenting business cases, invitations to tender and statements of requirements both orally and in writing.		Shortlisting & Interview
	Good written skills to write technical procedures, reports and documentation.		Shortlisting
	Excellent time management		Shortlisting
	Ability to schedule your own workload and prioritise your work.		Interview

	Essential	Desirable	Stage to be assessed
Training and Education/ Qualifications	A willingness to undertake further training and to learn and adopt new procedures as and when required.		Interview
	Ability to assimilate technical information and keep up-to-date in your field.		Shortlisting & Interview
	Degree with relevant IT/Computing content OR relevant professional IT qualifications and/or experience.		Shortlisting
		Information Security related qualifications: CISSP, CISM or similar	Shortlisting
		ITIL Foundation training and accreditation.	Shortlisting
Other	To observe the organisation's Equal Opportunities policy at all times.		Interview

Stages in assessment: **Shortlisting, Test (where appropriate) and Interview**

Conditions of Service

The appointment will be on a **full time, open ended** contract on **Management and Specialist Grade (salary, discretionary to salary per annum)*** at a starting salary commensurate with experience and qualifications.

*The appointment will be subject to the University's normal Terms and Conditions of Employment for **Academic and Related** staff, details of which can be found at:

<Terms and Conditions Link>

Informal Enquiries

Informal enquiries should be made to **<name>**, **<title>** by email at: **<email address>** or by telephone on **<telephone number>**.

Application

The closing date for receipt of applications is **<insert>**.

SFIA competencies

The SFIA (Skills Framework for the Information Age) framework from the British Computer Society defines core competencies for a range of IT related disciplines.

The core competencies for information security professionals are listed below:

- Demonstrates extensive knowledge of good security practice covering the physical and logical aspects of information products, systems integrity and confidentiality.
- Has expert knowledge of the employing organisation's security policies and all relevant legislation and industry trends which affect security within the defined scope of authority.
- Exhibits leadership qualities and is persuasive. Is familiar with the principles and practices involved in development and maintenance and in service delivery.
- Has extensive technical understanding and the aptitude to remain up to date with IT security and developments.
- Possesses a comprehensive understanding of the business applications of IT. Is effective and persuasive in both written and oral communication.
- Exhibits a meticulous method of working and attention to detail
- Demonstrates thorough knowledge of good security practice covering the physical and logical aspects of information products, systems integrity and confidentiality.
- Is thoroughly familiar with the employing organisation's security policies and all relevant legislation and industry trends which affect security within the defined scope of authority.
- Has extensive knowledge of the principles and practices involved in development and maintenance and in service delivery.
- Has good technical understanding and the aptitude to remain up to date with IT security and developments.
- Possesses a general understanding of the business applications of IT.
- Is effective and persuasive in both written and oral communication.

Collaboration between security administrators and academic researchers – UCL, case study

The UCL Security Working Group (SWG) partnered with UCL Human Factors researchers (led by Prof. Angela Sasse) from 2012, consulting regularly to ensure that the expectations of the user-facing password policy within the university were realistically achievable.

Related issues were presented by the SWG, and research expertise was shared by Prof. Sasse's group. Password policy was shared with researchers within the university.

Password policy was considered, but wider options for investment were also explored (such as alternative authentication technologies). After a series of meetings discussing organisation-wide password policies and authentication capabilities, business-driven decisions were presented which served to bound options for refining the password policy. Specific advice was tailored by researchers to match the university infrastructure (e.g. password length and complexity, password renewal intervals), based on research knowledge.

Viable changes were integrated into the password policy, reflecting the outcomes of discussions with researchers. These were discussed further with researchers, identifying potential future directions for investment and changes to policy, as well as challenges which may be faced as the organisation itself changed (in terms of population, available technologies, etc.).

This consultation explored ways to make better use of existing security systems, through communication with on-site researchers with related expertise. Consultation with researchers identified future challenges and informed procurement decisions. The process served to transfer expertise in both directions - researchers gained understanding of the deployment of authentication technologies and related security measures in practice within a large organisation, and SWG expanded understanding of the human factor of security. Both sides then demonstrated additional value to other functions within and outside the university. IT administrators developed a greater appreciation of the principles of human factors in security, and researchers gained insights that informed their research efforts at similar levels with other organisations.

Dialogue with researchers informed and influenced elements of authentication principles and password principles adopted at practitioner meetings. A new password policy developed, and was approved by the university's governance group.

Key Points

- Organisations can consider how cutting-edge or multi-disciplinary expertise already present within the organisation can be utilised in a way that benefits both security administrators and researchers.
- This case study also highlights that organisations should be aware of changes in the operating environment, and how these influence the bodies of expertise necessary to make informed decisions about policy and procurement.
- This is an example of an organisation actively identifying ways to minimise the impact of core security Responsibilities while maintaining an adequate level of security across the organisation (specifically the creation and management of suitably secure passwords which can be maintained over time by members of the organisation).