VERSION 1.0

NOVEMBER 30, 2018

THE UNIVERSITY
of EDINBURGH

INFORMATION SECURITY STRATEGY

2018 - 2023

CREATED BY: ALISTAIR FENEMORE

CHIEF INFORMATION SECURITY OFFICER

29/07/2019

TABLE OF CONTENTS

DOCUMENT MANAGEMENT

Version Control

Version	Author	Date	Changes
0.1	Michal Kopyra	21.03.2017	Document template
0.3	Alistair Fenemore	15/6/17	Incorporating review feedback
0.4	Alistair Fenemore	29/6/17	Incorporating peer review feedback from Tony Weir
0.5	Alistair Fenemore	05/10/17	Incorporating CIO feedback
0.6	Alistair Fenemore	31/1/18	Incorporating stakeholder feedback
0.7	Alistair Fenemore	31/8/18	Incorporating additional feedback
1.0	Alistair Fenemore		Further feedback

Approval

Title	Name	Date
CIO	Gavin McLachlan	14/11/18
ITC		17/12/18
KSC		18/1/19
University Executive		

EXECUTIVE SUMMARY

INTRODUCTION

The University, in common with any organisations who create, use or process digital information, faces an ever present and increasing threat of data compromise. High profile incidents and 'near-misses' demonstrate that this threat is real and must not be discounted, lest we risk material impact upon the day-to-day operation of the University and our well-deserved reputation. Additionally, global non-targeted cyber-security incidents could pose a threat if discounted. Although media attention invariably focuses on cyber incidents and breaches resulting from technical failure, University information also exists on other mediums, most obviously on paper, and this must also be protected. The controls required to secure all of the University's information effectively must therefore cater for all forms and include all elements of people, process and technology. Furthermore, we must counter the misconception that 'people are the weakest link' in managing information security. By providing the appropriate tools, procedures and knowledge to allow our people to operate successfully, they can become one of the strongest elements supporting our defence.

In addition, the University has taken on the responsibility of the CityDeal targets and will host large volumes of civic and commercial data as we aim to make Edinburgh the Data capital of Europe. To be successful, the University must be both trusted and worthy of that trust by the organisations sharing their data. To support this requirement, the CityDeal project are developing a detailed Information Governance approach that covers information security and information governance, particularly as they relate to ethical considerations on the use of personal data for the wider benefit of society. This strategy supports the information security aspects of that approach.

The University has taken on roles advising both Scottish and local government on information security including specific projects with the NHS, national Online Identity Assurance and State Sponsoring Cyber-attacks. It is critical that our Information security strategy and our best practice are of the highest quality.

The government, local councils, external partners and customers are looking to the University to be both a creator of data and leader in information security good practice, as well as a practitioner. Furthermore, as the first Scottish Academic Centre of Excellence in Cyber Security Research (ACE CSR), we have a leading role to play in shaping the future of best practice in cyber security. Finally, the University also holds large amounts of medical data used in clinical work and medical research that needs to be protected.

Although the University has operated a number of information security controls for some time, the appointment of a Chief Information Security Officer (CISO), formation of an Information Security Division and commitment of funding demonstrates the commitment the University has made to supporting improvements in this area. A material transformation of culture will take time and resource, particularly when the need to increase awareness and understanding of the risks and individual responsibilities across all of the University is required if we are all to be successful.

Positive information security risk management action needs to become an everyday part of how each member of staff, student, contractor, visitor and anyone else accessing or using University information, operates and acts. It is not something that someone else 'will do to' him or her, nor something that 'IT will do for them'. It is everyone's responsibility to understand the role they have individually, or collectively, in protecting University information, in all formats and mediums, and to implement appropriate controls to protect the confidentiality, integrity and availability of that information. Failure to do so could result in a range of impacts, from adverse publicity, loss of stakeholder confidence (further impacting ability to secure external grant funding or key industrial partnerships) impacting University or individual reputation, through to material regulatory censure and/or imposition of fines. In addition, any breach of information security could jeopardise our CityDeal ambitions as well as our medical research and clinical practices. Given the diverse nature of the University, it is clear that single, all-encompassing controls may not work for all areas in all circumstances. The focus should therefore be on the desired outcome that a particular control requirement will achieve rather than the specifics of implementation. By allowing some degree of flexibility where necessary, the common desired outcome can be met whilst minimising operational impact.

STRATEGY SUMMARY

This Information Security Strategy outlines the roadmap for the next 3 – 5 years by providing background details and highlighting potential threats and vulnerabilities that need to be identified, assessed, understood and countered. It outlines the overall Vision of where we need to be, detailing the drivers and objectives for this journey. It also provides strategic proposals under the key themes of Identify, Protect, Detect, Respond and Recover, with each area detailing individual objectives, approach and measures of success:

- Identify. Creation of a sustainable information security governance framework (including Policy, Standards and Processes) to provide a consistent approach to managing information security risks, both internally and at key third party suppliers.
- Protect:
    - Development of additional controls to manage user access and processes to introduce routine re-certification of required access permissions will ensure that individual users only have access to systems and data that they need to carry out their current role.
    - Effective mandatory user training, both generic and role specific, will increase overall awareness of information security risks and threats and individual responsibilities everyone has for managing information security.
    - Benchmarking our processes against external standards and obtaining industry and Government Certification where appropriate, will demonstrate our commitment to operate securely to external partners and stakeholders.
    - Effective patch management is key to countering many common internet based threats. By introducing robust processes and managing the full lifecycle of systems and software we can be confident that we are minimising potential threat vectors that could be easily exploited by malicious actors.

    - Cloud services need to be assessed and managed before we utilise them to process University information.
- Detect. Establishing a security operations capability will enhance our response to emerging threats within the University network and allow greater analysis of collected data.
- Respond and Recover. The ability to effectively respond to, and recover from, material information security incidents is critical to maintaining effective operations across the University and retaining stakeholder confidence.

Additionally, by leveraging relationships and building security partnerships with others, the University can be part of a larger community that protects itself and shares common experiences and lessons. Examples include CiSP, JISC, stronger relationships with Scottish (through the auspices of being a Cyber Resilience Catalyst as part of their cyber resilience action plan) & UK government (notably the NCSC as an ACE CSR), the NHS and other parties such as industrial partnerships and alliances. It is key that the University is seen, and acts as, a leading partner, visionary and positive agent in the area of Cyber Security within the HE sector and beyond.

Finally, it provides details on a proposed resource structure within the Information Security Division to support the delivery of the Vision, recognizing the contribution that local teams, such as Computing Officers, across the University also bring.

This strategy recognises that Higher Education is a unique sector, and the approaches taken to secure a corporate business of similar size and complexity will need to be adapted for the University environment – one solution will not meet all requirements. Through the adoption of an appropriate mix of people, processes and technology, the requirements for innovation and flexibility can be balanced against the requirement to protect our key information assets. When successfully implemented, the University will be better placed to address the challenges we need to overcome in our pursuit of growth and advancement targets and well founded to exploit the opportunities available to us.

INTRODUCTION

Background

As the University looks to expand our digital footprint and increase industrial partnerships, notably via the City Deal and increasing access to distance learners, the requirement to demonstrate to key stakeholders that we have robust, effective and sustainable controls in place grows. Investment in leading edge technology, enhanced processes and skilled resources will place the University in a strong position to counter both internal and external threats and allow us to exploit fully the skills and resources available across the University. Without this, there is a risk that we miss new opportunities, become susceptible to exploitation of our resources and remain vulnerable to an ever-increasing threat profile. Effective information security risk management controls will support the University's strategic progress. Additionally, with the volume of personal data processed across the University, be it for operational or research activities and increased focus on legislative requirements, such as Data Protection, we must be able to demonstrate that we have effective information security controls in place. With a conscious decision to move more services to be 'cloud based', there will be a need to amend our approach to counter any additional risks associated with this.

Context

We live in an increasingly inter-connected world. Our ability to deliver, innovate and grow is heavily dependent on the internet – a major tool of opportunity, but also, if left unchecked, a source of threat. Information security risk management cannot be an afterthought. It can be a business enabler and, if implemented effectively and in a timely manner, a business differentiator. Strategic direction and robust management of information security will provide the University with the chance to seize business opportunities that increase industrial partnerships and enhance our position. However, as our reliance on information systems and networks grows, so do the opportunities for those who would seek to maliciously compromise and exploit our assets, in either a targeted way or as a by-product of more general malicious activity (we get 'caught up' in wider attacks).

Threat Landscape

Different threat actor groups that may have a desire to disrupt the University have been identified and are detailed below. Their motivation, tactics and capabilities have been considered when developing this Strategy.

Cyber criminals

Individuals or groups who take advantage of the internet and internet related technologies to commit crime. The UK government has identified two types of cybercrime activity – cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crimes can only be committed using the internet whereas cyber-enabled crime relates to traditional crimes that are increased in scale, or reach, by exploiting the internet. Cybercriminals are financially motivated and vary in skill level and resources available. Organised criminal groups (OCGs) can be both highly skilled and well resourced, which makes them one of the top threat actors. As Cyber-Crime as a Service becomes increasingly available and cheap via the dark web, an increase in attacks against the University is highly likely as these factors open this option to a wider audience. Threats posed to University by such groups include:

- attempts to compromise University or partner IP
- access to computational facilities to support their criminal activities (as seen in late 2016 and again in early 2018, when we were compromised to process bitcoins), or as the source of attacks on other sites
- deployment of ransomware to disrupt operations or attempt to extract funds
- theft of personal data to undertake identity theft
- former disgruntled staff who have an ongoing grievance against the University

Hacktivists

Individuals or groups motivated by a political, social or religious purpose; for example, free speech, human rights or freedom of information. Hacktivist groups are often decentralised and made up of disparate individuals who share a similar viewpoint. Attacks are frequently disruptive in nature such as Distributed Denial of Service Attack (DDoS) but hacktivists are increasingly able to subject their victims to greater and more lasting attacks that include erasing or leaking sensitive information. Very much like cyber criminals, hacktivists can vary in skill level and resource availability. Hacktivist groups can contain thousands of members, many of whom are highly skilled and resourceful. Threats to the University come from groups such as:

- animal rights activists
- groups who object to our research partners (oil and gas companies, government departments etc)

Other groups

The threat landscape is continually evolving. New vulnerabilities, techniques and threat actors emerge and disrupt current conditions and ways of working. The groups outlined above are two of the better known and understood; however, we also need to consider some others:

- ‘Insiders’ employees who accidentally or maliciously cause cyber harm. Unintentional actions or omissions such as clicking on a phishing email, plugging in an infected USB stick, downloading unsafe content from the internet or ignoring an information security policy could result in similar outcomes as those posed by external cyber criminals or hacktivist. This could include individuals explicitly placed or targeted within the University by groups with a specific malicious agenda.
- A growing number of sophisticated, well-funded and mission specific threat actors have been observed and reported outwith the University. Such groups also include State sponsored actors and, whilst they may not target the University directly, there is still a

risk that we could be impacted by global attempts to exploit widespread vulnerabilities as demonstrated with the 2017 WannaCry ransomware attacks.

- State Sponsored actors are a very serious and growing concern, as they are increasingly using or outsourcing work to hacker organisations, which increases the effectiveness while creating a growing "economy" of hackers for hire or 'cyber-crime as a service'. Recently the University participated in discussions about the formational of a world-wide NGO called the International Centre for Cyber Peace aimed at exposing this activity and assisting victims. This initiative is sponsored by MasterCard and Microsoft.

All of these Groups utilise advanced and persistent techniques that require collective organisational countermeasures to provide an effective defence. We must therefore ensure that we have the correct spectrum of controls in place and that everyone knows their roles in implementing them.

Vulnerabilities

As the University moves forward, delivers, innovates and grows, our digital footprint will naturally increase. This will create new avenues that can be exploited and increases the potential for successful attacks that could result in a negative impact to our reputation, compromise our systems or data and adversely affect our staff, students and partnerships. We need therefore to consider the environment in which we will operate in the future.

Data Driven Innovation

The University's ambition through new initiatives such as the City Deal, to be a regional and global leader in Data Driven Innovation including ambitions to host, consult, analyze and innovate on a wide range of civic and commercial data means the University has to demonstrate an especially high level of maturity in Information Security and data ethics. We will operate as a center of best practice and innovation. Additionally, the presence of such data sets is likely to prove attractive to cyber criminals, increasing the risk of external attack.

Increasing volume of valuable data types

Research and innovation is at the forefront of the University's strategic vision and data will play a critical role to allow us to realise this. The increase in volume and variety of valuable data will introduce new risks to confidentiality, integrity and availability of this strategic asset, used for both operational and research activities. As we succeed through the CityDeal in deriving value from data, the data itself will become more valuable as an asset and thus potentially a more attractive target.

Increased online presence

We are a truly global University. As we increase our numbers of digital learners, our teaching becomes more dependent on key delivery technologies such as web and mobile. Whilst the use of these technologies will help us grow our student numbers and improve the accessibility of our services, the potential attack surface will also increase.   With an existing web estate that is diverse and disparate, we face challenges from legacy development that must also be addressed.

Growing range of devices

The number of networked devices is rapidly increasing. With a growing adoption of wearable technology and the Internet of Things (IoT), the number of devices connecting to our network will be greater than ever before. This increased connectivity will introduce new opportunities for attacks on the assets to which these devices connect.

Risk Assessment

By bringing the background, context, threat actors and vulnerabilities detailed above together, it is apparent that the University faces a real and ever evolving threat landscape. It is therefore essential that we manage this towards an acceptable level by operating a holistic, risk based response. The introduction of more rigour and structure, together with additional controls and enhancement of those that are already in place, will greatly improve the current information security risk management position and better support the University's aspirations.

STRATEGIC PROPOSAL

Our Vision

To be effective, it is critical that this Strategy supports the overall University Strategy. It must therefore have a meaningful Vision:

> Information security risk management is pervasive across the University with widespread awareness of the threats facing the University. Individuals understand their own roles and responsibilities and recognize the opportunities that effective information security risk governance can provide. Staff and students implement good information security risk management practices to support innovation and enable the development of flexible and agile business solutions. The University acts as a creator and practitioner of information security good practice.

Key Themes

To realise this Vision, measures will be implemented to address the following key functions:

Identify

Organizational understanding and awareness of information security to effectively identify and manage information security risk to our key information assets, be that data or services.

Protect

Appropriate controls and safeguards to create an environment in which our staff and students have the opportunity to achieve their objectives and the confidence to seize new initiatives whilst enabling the delivery of key business services.

Detect

Appropriate systems, capabilities, processes and procedures to detect information security events as early as possible.

Respond

Appropriate capabilities, processes and partnerships to take effective action against detected information security events that affects the University.

Recover

Systems, capabilities and processes to augment plans for business resilience and to restore any capabilities and/or key services that were impaired by an information security event in an efficient and effective manner.

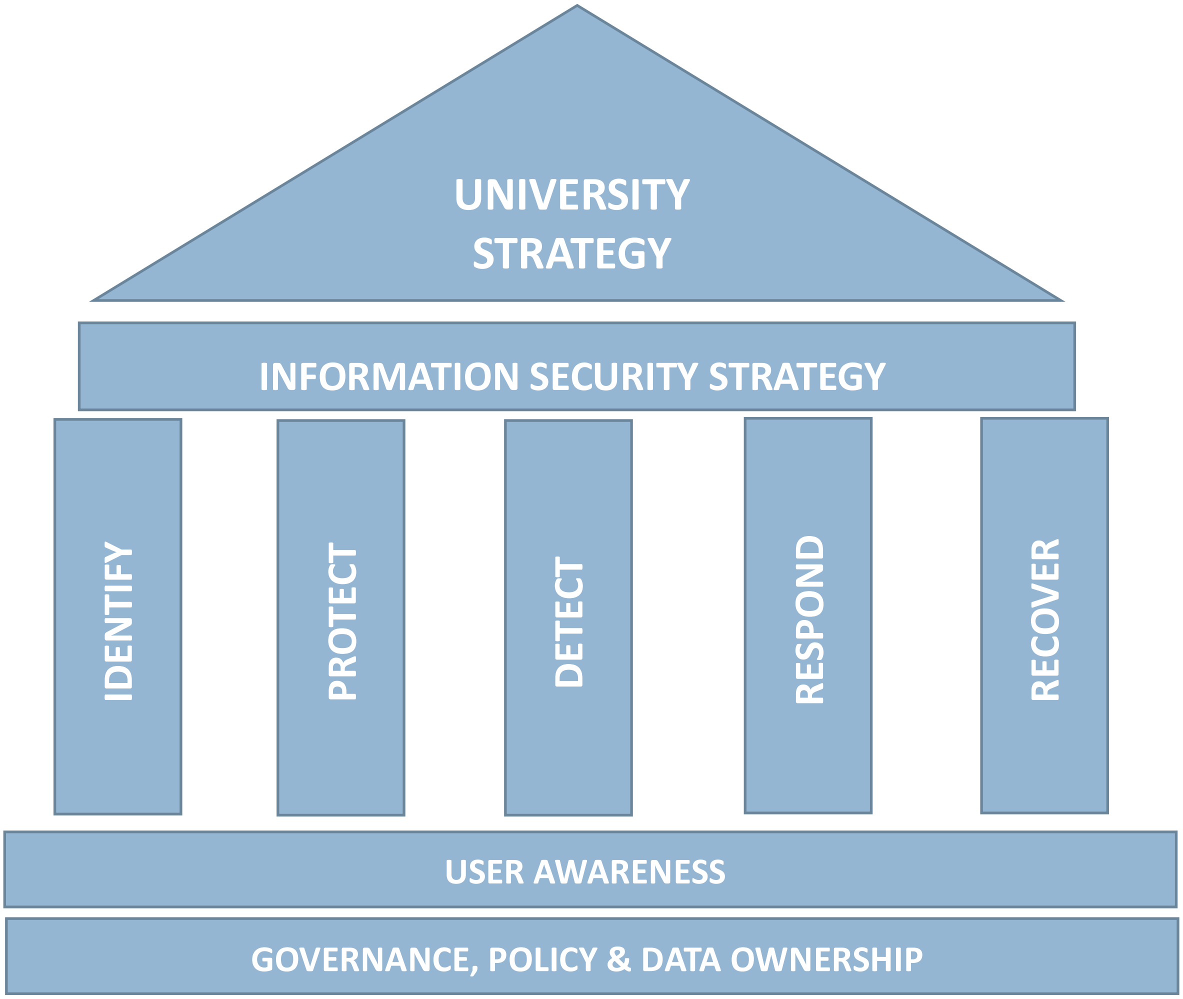
These key functions will be underpinned by supporting elements:

Governance, Policy and Data Ownership

It is essential that robust information security risk management governance and policy be in place to provide the requisite control framework that will allow the University to demonstrate *its cohesive approach to countering threats. Additionally, for each Golden Copy of key University datasets, a Data Steward will be appointed, their responsibilities defined and supporting guidance made available.*

User Awareness

Effective and sustainable user awareness is required so that everyone is aware of their individual contribution to managing information security risks in line with the University risk appetite.



Roles and responsibilities

Securing the University's information and systems requires a collaborative effort across the University. All staff, students, visitors and anyone accessing or using our information, in any format, have an important role to play in through adhering to key operational information security principles and controls. The specific responsibility varies according to a person's group:

Senior Management

The role and responsibility of senior management within each College and Support Group in information security is a critical one. Their primary responsibility is to identify and appropriately manage the organisational information security risks within their areas of responsibility. A Chief Information Security Officer (CISO) is in place to help achieve this objective at a University level. CISO will set out, and own, the vision, strategy and supporting information security policies for the University. The CISO's office will measure progress against the strategy, handle Information security incidents and measure compliance with the information security controls. Senior management will lead by example and will champion the adoption, implementation and compliance with information security risk management requirements and policies. Senior management must also understand that, if the University falls victim to a cyber-attack, they might be personably accountable for the consequences.

Staff

Staff are responsible for protecting and maintaining the Confidentiality, Integrity and Availability of all information assets they use, access, manage or own. Staff must comply with organisational information security policies and take reasonable steps to incorporate the appropriate level of security into all decisions and actions taken in line with the University's risk appetite. Staff must also take due care to help identify, escalate and manage information security risks by following the policies and procedures set out by senior management. These policies include, but are not limited to, Information Security and Data Protection.

Students

Students must take reasonable steps to understand the risks they face as individuals and act appropriately to protect their identities, credentials and devices as well as University information assets, facilities and services that they use. To support the achievement of this objective, it is essentials that students utilise tools and resources available to them and comply with University computer regulations and information security policies as required.

Data Stewards

Data Stewards will be formally assigned against each of the University's critical golden datasets. They will be responsible for ensuring that appropriate procedures are in place to manage the security and access processes in place to provide appropriate security of their data sets. They are also responsible for documenting the data under their care and for having controls in place to define and check data quality. Oversight of these roles lies with the Data Governance Group.

Specialist Resources

The CISO is responsible for establishing and maintaining a team of information security specialists who will provide support and guidance to assist staff and students to manage the information security risks facing the University on a day-to-day basis. This team will comprise dedicated resources working directly for the CISO, together with a wider 'virtual team' that will come from across the University. Where necessary, CISO will augment internal resources by engaging external subject matter experts who will provide bespoke advice and guidance. The CISO is also responsible for advising Senior Management on existing and emerging strategic information security threats and for creating and managing an overall information security risk management governance framework. The CISO's office will measure progress against the strategy, handle Information security incidents and measure compliance with the information security controls. Additionally, whilst not their primary role, there are a large number of people across the University who can influence the implementation of robust information security controls. This includes the Data Protection Officer, local Computing Officers acting as trusted advisors, data protection champions and Records Management.

Implementation

Against each Key Theme, three distinct elements have been identified:

Objectives

Objectives set out our target state goals and focus for the future by demonstrating what we want to achieve. (A summary of the Objectives is included in Annex A)

Approach

Approach outlines the steps that we are going to take to help us achieve our Objectives.

Measuring Success

Success measures provide a quantifiable way of tracking our actions and progress toward our Objectives over time. They help us understand our current position and enable us to share that position both internally and externally.

The following activities form the Information Security Strategy. Each plays an integral part in the overall journey towards our target state. Each theme will require work; some areas are already underway, some are in plan and some have yet to be fully scoped. As the threat landscape changes and expands, external monitoring will be undertaken to identify areas that are new, have changed or those that no longer present a material risk to the University. This portfolio of work will require resource, both funding and headcount and submissions for these will be made as part of the annual planning round.

1. Identify

1.1 Governance and Compliance: The policies, procedures, and processes to manage and monitor the University's regulatory, legal, risk, and operational requirements are understood and inform the direction of information security risk management.

Objectives:

1.1.1 Information security policies are developed, documented and embedded across the University.

1.1.2 Information security policy ownership has been assigned to appropriate stakeholders.

1.1.3 Compliance monitoring and reporting processes that support the information security activities are developed and embedded across the University.

Approach:

- *Consult and work with senior management and internal stakeholders to develop a set of information security policies tailored to the University strategic goals and risk profile.*
- *Take appropriate action to make information security policies easily understood and accessible to staff, students and external partners.*
- *Design and implement simplified compliance monitoring processes that enable regular reporting to KSC, Audit & Risk Committee and Court.*

Measuring Success:

- *Senior management have signed off documented Information.*
- *Senior management demonstrate continuous support for information security by promoting key policies and industry good practice.*
- *Ownership and accountability for information security policies assigned. Senior management, staff, students and other internal and external parties understand their individual and collective roles and responsibilities.*
- *Information security requirements and relevant policies communicated to staff, students and other internal and external parties. Regular communication channels are established.*
- *Information security policies are accessible to staff, student and other internal and external parties.*
- *Information security policies reviewed periodically.*
- *Continuous compliance monitoring practices adopted and used to monitor information security key performance indicators (KPI's).*
- *Reporting generated and shared with appropriate governance committees on a regular basis.*

1.2 Risk Management: The University information security risk appetite is agreed, clearly expressed and understood by all stakeholders. The combined information security risk facing the University is understood and processes to identify and manage this risk appropriately are established and embedded into Colleges and Support Groups.

Objectives:

1.2.1 The University information security risk appetite is determined, agreed and documented in line with the wider risk management processes.

1.2.2 The University has developed, documented and embedded a consistent way to assess information security risks across all its operations both internally and externally.

1.2.3 Processes to manage information security risks, including oversight, governance and regular reporting, are developed and embedded across the University.

Approach:

- *Consult and work with senior management to determine and document the University information security risk appetite.*
- *Develop and document a consistent way to identify and assess information security risks and communicate them with the relevant stakeholders.*
- *Design and implement simplified risk management processes that enable effective oversight and regular reporting.*

Measuring Success:

- *The University has a clear understanding of its information security risk appetite. This is documented, signed off by senior management and communicated to staff, students and other internal and external stakeholders.*
- *A consistent process to identify and assess information security risks documented. Risks identified early, documented and monitored. Reports shared regularly with senior management.*
- *Known, accepted risks reviewed regularly and reassessed to validate the level of risk posed to the University in line with the agreed risk appetite.*

1.3 Third Party Management: Information security policies and processes are in place to identify, assess and understand supply chain risks at key suppliers, including but not limited to screening, on boarding and periodic information security reviews. Once identified, these risks are documented, monitored, regularly reviewed and reported.

Objectives:

1.3.1 Key third party suppliers are aware of the University information security risk management requirements and are required to recognise, and where practicable comply with, the University information security policies and procedures.

1.3.2 Key third party supplier information security risks identified, assessed and documented as part of due diligence processes prior to contractual agreements.

1.3.3 Key third party supplier information security risks monitored, regularly reviewed and reported on. The frequency of these activities depends on the associated level of assessed risk.

Approach:

- *Communicate the University information security risk appetite and the relevant information security policies and procedures with key third party stakeholders.*
- *Make the relevant information security policies and procedures accessible to key third party stakeholders.*
- *Include our mandatory security requirements/clauses in procurement documents and contract documents at an early stage in the procurement process.*
- *Develop, document and implement a sustainable process to identify and assess information security supply chain risks at key third parties in a consistent manner.*
- *Consult and work with internal and external groups to develop processes and procedures to monitor, review and report on information security supply chain risks at key third parties.*

Measuring Success:

- *University information security requirements and policies are communicated to and accepted by third party stakeholders prior to engagement to influence which third parties we are prepared to collaborate with.*
- *A consistent process documented to identify and assess third party supply chain information security risks. Risks identified early, documented and monitored. Reports regularly shared with senior management.*

- *Third party supply chain information security risks are regularly reviewed and reassessed as part of the supply assurance practices to validate the level of risk posed to the University in line with the agreed information security risk appetite.*

2 Protect

2.1 User Access: Access to information assets and associated facilities is limited to authorised users, processes or devices in line with Role Based Access Control (RBAC) principles

Objectives:

2.1.1 Identities and credentials for authorised devices and users are managed centrally using specialist technical solutions such as an Identity and Access Management System (IDAM) and in line with Role Based Access Control (RBAC) principles.

2.1.2 Physical and remote access to information assets managed securely.

2.1.3 User access to systems and data is reviewed on a regular basis to ensure that unnecessary access is removed.

Approach:

- *Centralise control to manage identities and credentials for devices and users in a secure and automated manner by implementing specialist technical solutions such as an Identity and Access Management (IDAM) System.*
- *Adopt and embed industry good practice and Role Based Access Control (RBAC) principles to control and manage user access to information assets, services and facilities.*
- *Implement processes and procedures to review user access permissions including privileged access on a regular basis.*

Measuring Success:

- *Specialist tools implemented to manage identity and access to information assets, services and facilities in a centralised and automated manner. These tools configured according to industry good practice.*
- *Access permission both logical and physical granted in line with Role Based Access Control (RBAC) principles and reviewed on a regular basis.*
- *Privileged access requires asset owner approval and review on a regular basis, no less than annually.*
- *Users only retain access required for their current roles, with access reviewed when changing roles.*

- *'Leavers' access to University systems and information is removed as soon as practicable after their relationship with the University has finished.*

2.2 Information Security Awareness and Training: University staff, students and other users of University systems and data receive appropriate information security awareness training to perform their duties and responsibilities consistent with organisational and legal policies, procedures, and agreements.

Objectives:

2.2.1 Senior management given an adequate level of information security training to understand their roles and responsibilities.

2.2.2 Staff, students and other internal and external users accessing University information provided with an appropriate level of information security training and/or access to relevant information.

2.2.3 Privileged users given enhanced information security training to ensure they understand the additional responsibilities related to their roles.

Approach:

- *Mandate information security user awareness training for all staff and contractors who have access to University information assets as part of local induction processes and at regular intervals thereafter.*
- *Communicate information security requirements, policies and procedures to all internal and external stakeholders.*
- *Develop tailored information security training material for key user groups including but not limited to senior management, staff, students and privileged users. Training to recognise the holistic nature of effective risk mitigation and to encompass the range of people, process and technology inputs required to deliver required outcomes.*
- *Make training material easily accessible by utilising web based digital learning technology.*
- *Develop and implement a process to enable organisation wide communication of relevant information security messages.*
- *Develop an effective reporting mechanism to enable tracking and reporting of completion rates of mandatory information security awareness training.*

Measuring Success:

- *Information security training completed by users in the form of induction training and annual refresher training.*

- *Information security training is readily available by utilising web based digital learning technology and other centralised resources.*

2.3 Consulting Services: Specialised information security capability is established to provide consulting and advisory services to the business.

Objectives:

2.3.1 The University has a specialist information security function with resources and capability to provide internal consultancy to projects and teams across the Colleges and Support Groups.

2.3.2 The Information security function resourced appropriately to be able to provide ad hoc consultancy services when needed.

2.3.3 External partnerships established to provide additional information security capabilities when required. This includes but is not limited to security consultancy and security testing services.

Approach:

- *Invest in specialist information security resources to form an information security function capable to support the University vision.*
- *Develop external partnerships to help provide advice, support and supplement internal capabilities where appropriate.*

Measuring Success:

- *Appropriate internal information security consultancy provided to projects and teams throughout the University when needed.*
- *The University maintains external partnerships to secure support and supplement its own internal consulting capabilities when required.*

2.4 Certification and Benchmarking: University information security policies procedures and practices are aligned, compliant with and/or certified by, national and international standards for information security. This includes but is not limited to Cyber Essentials/ Cyber Essentials Plus or ISO/IEC 27001:2013. Regular benchmarking assessments are carried out to compare information security metrics against a peer group and/or industry good practice.

Objectives:

2.4.1 University information security policies, procedures and processes aligned, compliant or certified to industry good practice, national and international standards such as Cyber Essentials/Essentials Plus, ISF Standard of Good Practice, NIST or ISO/IEC 27001:2013.

2.4.2 University processes are developed and implemented to regularly validate alignment, compliance or certification with chosen standards for example, Cyber Essentials/ Cyber Essentials Plus.

2.4.3 Internal and/or external benchmarking assessments carried out to compare information security metrics against a peer group and/or industry good practice.

Approach:

- *Carry out an assessment to understand which standards the University must comply with, together with ones that add value. Document the outcomes of the assessments.*
- *Align, comply or seek certification for information security policies, procedures and process for the chosen (must/want) national and international standards in line with the initial assessment/s.*
- *Develop and implement processes and procedures to regularly validate alignment, compliance and/or certification with chosen standards*
- *Schedule internal and/or external benchmarking assessments to compare information security metrics to a peer group and/or industry good practice.*

Measuring Success:

- *Achieve and maintain an appropriate level of alignment with national and international standards based on business requirement and in line with the initial assessment.*
- *Reassess requirements and needs regarding national and international standards on a regular basis, at least annually.*
- *Carry out periodic internal and/or external benchmarking assessments to compare information security metrics to a peer group and/or industry good practice.*

2.5 Information Security Working Group: The information security-working group (ISWG) acts as a focal point for technical and non-technical information security matters across the University. The group is a platform for sharing and discussing information security good practice and makes recommendations on the improvement of the overall security posture of the University and its associated groups and communities. The ISWG provides regular updates to ITC.

Objectives:

2.5.1 The ISWG is established and its terms of reference defined, agreed and documented with relevant stakeholders.

2.5.2 The group meets on a regular basis. Meeting minutes and actions documented and archived.

2.5.3 Terms of reference reviewed at least annually to validate their appropriateness against actions taken during review period.

2.5.4 The ISWG reports relevant information security updates to ITC for information, review and/or approval as required.

Approach:

- *Maintain the ISWG consisting of representatives from key business units.*
- *Define, agree and document group's terms of reference.*
- *Meet as a group on a regular basis in line with ITC meeting schedule.*
- *Develop and implement a process to review the appropriateness of terms of reference and actions taken during review period.*

Measuring Success:

- *The ISWG formed; its terms of reference documented and communicated with all stakeholders.*
- *Meetings held and attended by representatives from key business units. Any agreed actions documented, escalated to ITC as required and archived.*
- *Annual review of group's terms of reference and key actions taken is undertaken.*

2.6 Patch Management: A comprehensive patch and update management strategy, together with supportive processes, is established to identify, evaluate and apply required security patches and updates while ensuring the availability of key business resources including information systems and applications. This will help ensure that equipment remains fit for purpose and provides the expected level of protection throughout its in-service lifecycle and will identify when it is likely to become obsolete or out of support as retaining such equipment introduces additional risks.

Objectives:

2.6.1 A process is in place to identify, evaluate and apply security patches and updates in a timely manner for key business resources including information systems and applications.

2.6.2 Key business resources including information systems and applications kept up to date with the latest security patches and updates.

2.6.3 A process is in place to manage the full lifecycle of key assets to include upgrades, end of life approach and secure disposal.

Approach:

- *Define, agree and document the University patch management strategy.*

- *Establish and implement supportive management processes to identify, evaluate and apply security patches in a timely manner.*
- *Communicate patching strategy and supportive management processes with the relevant stakeholders.*
- *Regularly review and report on patching status of key business resources.*

Measuring Success:

- *Patch management strategy defined, documented and communicated with the relevant stakeholders.*
- *Supportive processes embedded and operate as intended.*
- *Regular reviews conducted to assess the effectiveness of the patch management strategy and its supportive management processes.*
- *Management information on patch status of key business resources shared with the relevant stakeholders at least quarterly.*
- *Key business resources, including information systems and applications, kept up to date with the latest patches in line with the patch management strategy.*

2.7 Cloud Services: Cloud security requirements, policies and procedures are defined to guide the procurement, implementation, management and security of cloud services. University requirements, policies and procedures are communicated with the relevant internal stakeholders and external third parties.

Objectives:

2.7.1 The University cloud security requirements, policies and procedures defined, documented and communicated with the relevant stakeholders including external third parties.

2.7.2 Cloud services procured, implemented, managed and secured in line with University cloud security requirements, policies and procedures.

Approach:

- *Define, agree and document cloud security requirements, policies and procedures for procurement, implementation, management and security of cloud services.*
- *Include our information security requirements and contract clauses in the procurement process early on.*
- *Communicate cloud security requirements, policies and procedures with the relevant internal and external stakeholders.*
- *Carry out periodic compliance reviews to verify compliance with cloud security requirements, policies and procedures.*
- *Conduct regular reviews of cloud security requirements, policies and procedures to assess their effectiveness and appropriateness.*

Measuring Success:

- *Cloud security requirements, policies and procedures defined, documented and communicated with relevant stakeholders.*
- *Periodic compliance reviews carried out to verify compliance with cloud security requirements, policies and procedures.*
- *Regular reviews conducted to assess the effectiveness of cloud security requirements, policies and procedures.*
- *Compliance with cloud security requirements, policies and procedures and their effectiveness is included in management information reporting.*

3. Detect

3.1 Security Operations: Technical information security solutions and supportive processes are in place to manage information security operations and provide capabilities to monitor assess and defend information systems and networks.

Objectives:

3.1.1 Network segmentation and supportive network security controls implemented to improve performance and increase resilience and security of the network.

3.1.2 Centralised technical operations function established to monitor assess and defend information systems and networks.

3.1.3 Security Information and Event Management (SIEM) solution implemented to provide real-time correlation and analysis of security events generated by information systems and networks. This will include feeds from monitoring tools such as Intruder detection/prevention systems, netflow analysis etc.

3.1.4 Tools, services and processes are implemented to provide threat intelligence feeds and an automated threat monitoring capability across a range of sources including but not limited to UK-CERT and Cyber-Security Information Sharing Partnership (CiSP) operated by the NCSC.

3.1.5 Security testing scope is developed and testing schedule agreed to carry out regular security assessments on information systems and networks utilising both internal and external capability.

Approach:

- *Review and assess the current design and architecture of the network. Implement improvements and/or additional network security controls where appropriate.*
- *Invest in a technical security operations function with capability to monitor, assess and defend information systems and networks.*

- *Purchase and implement specialist security tools including but not limited to Security Information and Event Management (SIEM) used by the technical security operations function.*
- *Purchase and implement specialist security services including but not limited to threat intelligence used by the technical information security operations function.*
- *Develop and document an information security testing scope that covers key information systems and networks and follows a regular testing schedule.*

Measuring Success:

- *Network performance, resilience and security have increased because of network segmentation and the implementation of supportive network security controls such as Intrusion Detection and Prevention System (IDPS).*
- *Technical operations function formed and has resourcing capability consisting of skilled specialist staff to assess and defend information systems and networks.*
- *Security tools including but not limited to Security Information and Event Management (SIEM) purchased and implemented to enable technical security operation staff to carry out real-time correlation and analysis of security events.*
- *Security services including but not limited to threat intelligence feeds purchased and implemented into the technical operation function.*

4. Respond

4.1 Incident Response: Information security incident response processes and procedures are defined, documented and communicated to all relevant stakeholders. Strategic partnerships are in place to provide external advice, support and to supplement internal capability where appropriate. Regular testing and training takes place to ensure all stakeholders are confident in their responsibilities and required actions and in the effectiveness of the plan.

Objectives:

4.1.1 Information security incident response processes and procedures are developed, documented, implemented, tested and communicated with the relevant stakeholders.

4.1.2 Information security incident response training is provided to those with active response roles.

4.1.3 Strategic partnerships with external stakeholders are developed.

4.1.4 Information security incident response activities are improved by investigations into root cause and by incorporating lessons learned from previous detection and/or response activities.

Approach:

- *Develop, document and implement a University wide information security incident response process and communicate it with the relevant stakeholders.*
- *Establish internal information security incident response capability in the form of specialised incident response team.*
- *Establish internal information security digital forensic capability in the form of specialist equipment and resource.*
- *Develop and provide relevant information security incident response training for those with active response roles.*
- *Develop external partnerships to help advice, support and supplement internal capabilities where appropriate.*

Measuring Success:

- *Information security incident response processes defined, documented, tested and communicated with the relevant stakeholders.*
- *Specialist information security incident response team is in place with team members trained and aware of their roles and responsibilities.*
- *The University maintains external partnerships to support and supplement its own internal incident response capabilities when required.*

5. Recover

5.1 Recovery Planning: Information security recovery processes, procedures, systems and capabilities are in place and known by the appropriate stakeholders.

Objectives:

5.1.1 Information security recovery processes and procedures are developed, documented and implemented. Key information security processes and procedures shared with the appropriate stakeholders.

5.1.2 Suitable training provided to those with active recovery roles.

5.1.3 Recovery activities improved by incorporating lessons learned from previous recovery activities.

Approach:

- *Develop, document and implement University wide recovery processes and procedures. Communicate them with the appropriate stakeholders.*
- *Establish internal information security recovery capability in the form of specialised recovery team.*
- *Develop and provide suitable recovery training for those with active recovery roles.*

Measuring Success:

- *Information security recovery processes and procedures defined, documented and communicated with the relevant stakeholders.*
- *Specialised information security recovery team is in place with team members trained and aware of their roles and responsibilities.*

6. Information Security Division – Delivery Structure

To deliver each activity detailed against the key themes, the Information Security Division will be structured into three main teams – Consult, Govern and Operations. Team responsibilities will adapt as required, with resource flexing to areas of greatest need, depending upon prevailing circumstances. Effective response to any material information security incident or an incident with an information security impact will take precedence over non-urgent activity. Cases of conflicting resource requirements will be escalated to CISO who will arbitrate as required. As stated previously, the delivery of a sustainable information security risk management framework also requires the ongoing delivery of services by other Divisions in ISG, notably ITI, ADO, LTW and USD. Additionally, stakeholders in each of the Colleges and Support Groups provide valuable resource and local knowledge that help ensure a holistic view and implementation of effective controls.

6.1 **Consult Team:** Core activities for the consult team will include:

- Support to projects
- First point of contact for general, ad-hoc enquiries and requests for support
- Provision of information security awareness across the University
- Incident support to include digital forensics when required

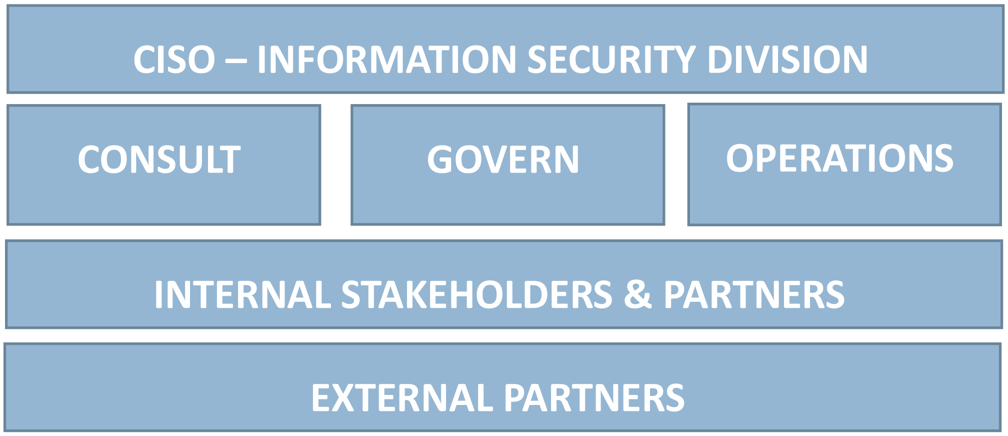
6.2 **Governance Team:** Core activities for the Governance team will include:

- Management of information security governance framework to cover policy, standards, procedures and guidance
- Management of University Computing Regulations to ensure alignment with Policy

- Reviews to confirm status of Information Security Policy compliance across the University
- Risk reporting
- Development and ongoing management of suitable KPI's, certification process and control framework
- Management of Information Security Working Group
- Management of Information Security Certification (ISO 27001; Cyber Essentials etc)

6.3 Operations Team: Core activities for the Operations team will primarily be one of co-ordination with other Divisions across ISG who undertake or deliver a 'core' security service such as provision of user access or management of network security controls. The activities include:

- Management of security testing, including ownership of supplier framework
- Incident management co-ordination
- Liaison with internal and external stakeholders and partners


CISO – INFORMATION SECURITY DIVISION
CONSULT
GOVERN
OPERATIONS
INTERNAL STAKEHOLDERS & PARTNERS
EXTERNAL PARTNERS

Annex A – Summary of Objectives

Key Theme	Objectives	Summary	Implementation Starts	Funding Requirements
IDENTIFY	Governance & Compliance	Information Security Policy has been developed and assigned an owner (1.1.1 and 1.1.2)	2017	In place
		Compliance monitoring and reporting processes and resource are in place (1.1.3)	2019	To be sought for additional resource for CISO
	Risk Management	Information security risk appetite has been set and agreed (1.2.1)	2018	From CISO budget
		Development of risk assessment methodology (1.2.2)	2018	From CISO budget
		Development of risk management and reporting processes (1.2.3)	2018	From CISO budget
	Key Third Party Supplier Management	Key third party suppliers are aware of University information security risk management requirements (1.3.1)	2019	To be sought and work with Procurement
		Key third party supplier information security risks are assessed (1.3.2)	2019	To be sought
		Key third party supplier information security risks are monitored and reported (1.3.3)	2020	To be sought

PROTECT	User Access	Manage user access via IDAM in line with RBAC principles (2.1.1)	2019	Initially from CISO budget
		Manage access securely (2.1.2)	2019	To be sought
		User access is reviewed regularly (2.1.3)	2019	To be sought
	Awareness and Training	Senior Management receive information security training (2.2.1)	2017	From CISO budget
		Information security training is available (2.2.2)	2017	In place
		Users with enhanced access receive additional, role specific training(2.2.3)	2018	From CISO budget
	Consulting Services	Specialist internal information security resource is in place (2.3.1)	2017	In place
		Information Security function is effectively resourced (2.3.2)	2017	In place
		External partnerships are in place as required (2.3.3)	2017	In place and ongoing
	Certification & Benchmarking	University Policies are aligned to appropriate industry good practice and/or international standards (2.4.1)	2017	In place
		University policies are subject to ongoing validation (2.4.2)	2018	From CISO budget

		Information security metrics are subject to benchmarking assessments (2.4.3)	2018	From CISO budget
	Information Security Working Group (ISWG)	ISWG is established (2.5.1)	2017	In place
		ISWG meets regularly (2.5.2)	2017	In place
		ISWG ToR reviewed regularly (2.5.3)	2017	From CISO budget
		ISWG provides reporting to ITC (2.5.4)	2017	In place
	Patch Management	A patch and update management strategy is in place (2.6.1)	2018	To be sought
		Key resources are kept up to date (2.6.2)	2018	To be confirmed as BAU process for managing areas
		A process to manage the full lifecycle of information assets is in place (2.6.3)	2019	To be confirmed as BAU process for managing areas
DETECT	Security Operations	Network segmentation and supportive controls are deployed (3.1.1)	2020	To be sought – linked to Network Replacement
		Centralised security operations function is established (3.1.2)	2018	Initial funding agreed
		SIEM solution is implemented (3.1.3)	2019	Initial funding agreed

		Threat intelligence and threat monitoring is implemented (3.1.4)	2018	Initial funding agreed
		Security testing is scoped and undertaken (3.1.5)	2018	From CISO budget
RESPOND	Incident Response	Information security incident response processes are developed and implemented (4.1.1)	2018	From CISO budget
		Information security incident response training is implemented (4.1.2)	2018	From CISO budget
		Strategic external partnerships are established (4.1.3)	2018	Started and ongoing
		Root cause analysis and continuous improvement is embedded (4.1.4)	2019	From CISO budget
RECOVER	Recovery Planning	Information security recovery processes are developed and implemented (5.1.1)	2018	From CISO budget
		Training is provided to those involved in recovery activities (5.1.2)	2018	From CISO budget
		Recovery activities are improved by identifying areas of weakness (5.1.3)	2018	From CISO budget
Information Security Division Structure	Team Composition	Division comprises Consult, Govern and Operations teams (6.1 – 6.3)	2019	Additional resource to be sought via funding round