Information Security Policy (Revision 1)

of

University of Kelaniya

Table of Content

1. Introduction

Information is a vital asset to any organisation, especially to a knowledge-driven organisation such as the University of Kelaniya, where teaching and learning, research, administration and management increasing depend on Information Technology (IT) based systems. This makes it essential to enhance the security and reliability of IT-based systems and infrastructure that form these critical services. The objective of the Information Security Policy of the University of Kelaniya is to ensure that all information assets on which the university depends are adequately protected. Achieving this largely depends on staff, students and other relevant parties working diligently in accordance with policy guidelines.

2. Purpose

The purpose of this Policy is to:

1. Protect the confidentiality, integrity and availability of the university's information;
2. Take a considered and risk-based approach to information security management;
3. Establish a security-aware culture within the university, ensuring that all involved have the skills and awareness to manage and secure information;
4. Give assurance to the university and 3rd parties that information is appropriately protected;
5. Respond to, manage and learn from information security incidents to reduce the likelihood and impact of incidents; and
6. Enable continuous improvement in information security.

3. Scope

Information Security covers the protection of all forms of information to ensure its confidentiality, integrity and availability. This includes but is not limited to information stored or processed on computers, transmitted across networks, printed or written on paper, and accessed via personal devices. This Policy applies to:

1. Everyone who accesses university’s information assets. This includes staff, students, and other parties who use information asset of the university;
2. Technologies or services used to access or process information assets of the university;
3. Information assets processed in relation to any function of the university;
4. Information assets that are stored by the University or an external service provider on behalf of the university;
5. 3rd party, public, civic or other information that the university is storing, curating or using on behalf of another party; and
6. Internal and/or external processes that are used to process, transfer or store university information.

4. Definitions

Information asset: An item or body of information, an information storage system or an information processing system that is of value to the university

Confidentiality: Ensuring that information is only available to authorised users

Integrity: Ensuring that information is accurate and fit for purpose

Availability: Ensuring that information is available when and where it is needed

Critical system: A system whose failure may result in injury, loss of life, loss of ability to operate or very high costs for the organisation using that system

ICT Centre: Information and Communication Centre of the University of Kelaniya.

Faculty ICT Centres: ICT Centres of faculties which are located outside of Dalugama premises. These may manage their respective faculties' systems and networks in collaboration with the ICT Centre of the university.

5. Policy Statement

1. This set of policies has been approved by the Council of the University of Kelaniya and forms part of the university's policies and procedures. It is applicable to and is to be communicated to staff, students, and other parties who will have access to the IT systems of the university

2. This Policy and associated guidance shall be reviewed and updated regularly to ensure that they remain appropriate in the light of any changes in technology, the law, or university policy

3. Management and integrity of central computing servers, systems, core network switches, backup systems, and the overall network infrastructure interconnecting these systems is the responsibility of the ICT Centre

4. A member of staff or student shall never attempt to compromise the security of the internal systems of the university

5. All users have a responsibility to report promptly (to the ICT Centre) any incidents which may have an information security implication for the university

6. Specialist advice on information security shall be made available throughout the university by the ICT Centre

7. Every effort shall be taken to safeguard user data and information of users residing in the university's IT system. In the event of information loss, the university will make every attempt to correct conditions and restore losses. It may also undertake disciplinary action if subsequent investigations find willful negligence on the part of the responsible staff. However, the university is not liable for the loss of such data and information.

8. A formal complaint should be made to the Director/ICT Centre if users suspect that their personal information has been accessed without authorisation. The ICT Centre should investigate such complaints and inform the outcome, and report to the Vice-Chancellor if the university's rules and regulations are found to be violated

6. Compliance

1. All faculties, departments, centres, units and administrative branches within the university must comply with this Information Security Policy. The responsibility for compliance lies with the appropriate Dean of the faculty, Head of the department, Head of the unit/centre, Officer in charge of the administrative branch

2. This policy sets out the responsibilities of all staff, students and third parties concerning their use of the university's IT-based systems and information assets. Any individual who accesses the university systems and/or data shall agree to comply with the Information Security Policy

3. Before any new critical system is introduced and connected to the network, a risk assessment process will be carried out to determine the appropriate level of security measures to be applied by the ICT Centre

4. All of the information systems of the university shall be operated and administered in accordance with relevant procedures, and the university may at any time monitor compliance with written authorisation of the Vice-Chancellor if there are reasonable grounds to believe that a violation of university policy has taken place

7 Users of IT-based Systems in the University

1. All users must comply with the Information Security Policy of the university. This requirement forms part of the university's terms and conditions of employment, and new employees will be notified of the policies when they sign their contract with the university

2. Breaches of this Information Security Policy and/or associated procedures shall result in potentially disciplinary issues and may lead to action being taken in accordance with the university's disciplinary procedures

3. All users shall be provided with awareness and to educate them regarding the range of threats, the appropriate safeguards, and the need for reporting suspected problems

4. The university is committed to provide training to all users of new systems to ensure that their use is both efficient and does not compromise Information security

5. Training will be made available to the systems management staff where appropriate to support them in maintaining their knowledge of current threats and information/IT security techniques

6. By default, accounts will be disabled 12 months after a member of staff or 6 months after a student leaves the university unless a separate temporary agreement is in place

7. Leaving users must return all information assets and equipment belonging to the university prior to departure unless otherwise agreed with the faculty, department, centre/unit or administrative branch responsible for the asset

8 Use of IT Equipment and Access Control

1. Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users' access rights match their authorisations

2. All users shall have a unique identifier (KelaniNet ID) for their personal and sole use to access university information services as appropriate. Personal user IDs must not be used by anyone else, and associated passwords shall not be shared with any other person for any reason. Shared accounts will only be allowed for special purposes and with restricted functionality. Such accounts will be disabled when deemed necessary by the ICT Centre in conjunction with the service owner

3. Password management procedures will be maintained to ensure the implementation of the requirements of the Information Security Policy and to assist both staff and students in complying with best practice guidelines

4. Access control standards will be maintained for all information systems at an appropriate level for each system, which minimises Information security risks yet allows the activities of the university to be carried out without undue hindrance

5. Access to all information systems must be authorised by the staff responsible for the system, and a record must be maintained of such authorisations, including the appropriate access rights or privileges granted

6. Procedures will be maintained for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff changes their role, or staff or students leave the university

7. IT equipment and other physical resources must be safeguarded appropriately – especially when left unattended

8. Staff must take reasonable steps to ensure that data held electronically are not vulnerable to theft or inadvertent disclosure to unauthorised users. These include locking a workstation if it is to be left unattended

9. The university installs protection against malicious software and computer viruses, where appropriate, on its computer systems. Users of these systems must not interfere with or prevent the operation of anti-virus protection. Care must be taken in this regard when transferring data to or from systems outside of the university network – including the transfer of data from home computers

10. Staff must take appropriate precautions to ensure that the risk of loss or damage to information is minimised. These precautions must include adequate backup and contingency arrangements for individual, local and centrally-run information systems

11. Care must be taken when transporting files on removable media (e.g., external hard disks, CDs, DVDs and USB flash drives) to ensure the safety of the media as well as the information it contains

12. Staff are only allowed to install permitted software onto the university's IT equipment

13. Any computer equipment in general office environments should be secured behind locked doors or protected by user log-out and or password-protected screensavers whenever it is left unattended and outside of general office hours

14. Desktop machines in public areas should contain a device or mechanism for securing and protecting the main components and contents of the computer from theft

15. Any portable equipment (such as laptops, memory sticks, tablets, PDAs, etc.) should use a log-on or power-on password wherever possible. Any unattended portable equipment should be physically secure, for example, locked in an office or a desk drawer. When being transported in a vehicle, they should be hidden from view. Staff should avoid storing sensitive information on portable equipment whenever possible

16. Staff who store confidential information on university-owned portable equipment must ensure that such data is thoroughly and securely cleansed from that equipment when they leave the university's employment

17. All third parties who access or use the university's hardware, software or sensitive information must agree to follow this Information Security Policy

9. Information Handling

9.1 Information Assets and Relevant Systems

1. An inventory will be maintained of all the university's major information assets, and the ownership of each asset will be clearly stated

2. Within the information inventory, each information asset will be classified according to sensitivity

3. When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted

4. The university advocates a clear desk and screen policy, particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential information is processed or viewed should be placed in such a way that unauthorised persons cannot view them

5. The backing-up of the university's information assets and the ability to recover them is an important priority. Respective 'owners' of systems are responsible for ensuring that the frequency of such backup operations and the procedures for recovery meet the university's business needs. Backup media must be removable and stored in an area remote from the physical system backed up. In the case of critical information systems where 24/7 service is required, consideration must be given to deploying fault-tolerant, high availability equipment

6. All information used by the university must be managed appropriately in line with the Document Management policy of the university

9.2 Electronic Communication

1. All forms of electronic communication, including email, digital collaboration platforms, social media, etc., are not entirely secure medium. Users should be conscious of this and consider how others might use electronic communication. It should be noted that messages can easily be taken out of context; once a message is sent, the user cannot control what the recipients might do with it; and that it is very easy to forward large amounts of information

2. Similarly, users should not necessarily trust what is received - in particular, users must never respond to a message request to give a username or password

3. Email and social media must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure confidentiality: that it is correctly addressed, intended recipients are authorised to receive it, and passwords are used to protect attached documents where required

4. Users should consider the security implications of any information they put on the university websites, and the university reserves the right to remove any material which it deems inappropriate, illegal or offensive

5. Users shall not in any way use web space to publish material that undermines Information security at the university. In particular, making information available about how Information security is implemented at a practical level, or any known weaknesses

6. Email addresses and fax/telephone numbers should be checked carefully prior to transmission, especially where the information content is confidential or sensitive or where the disclosure of email addresses or other contact information to the recipients is a possibility. The attachment of data files to an email is only permitted after confirming the confidentiality classification of the information being sent and checking that the document will have been scanned for the possibility of a virus or other malicious code

7. Information received via electronic communication must be treated with care due to its inherent information security risks. File attachments will be scanned for possible viruses or other malicious code

9.3 Encryption

1. A policy/guideline on encryption controls will be developed with procedures to provide appropriate levels of protection to sensitive information
2. Procedures shall be established to ensure that authorised staff may gain access, when needed, to any critical information being held in encrypted form
3. The confidentiality of information being transferred on portable media or across networks must be protected by using appropriate encryption techniques
4. Encryption shall be used whenever appropriate on all remote access connections to the network and resources of the university
5. A procedure for the management of electronic keys to control both the encryption and decryption of sensitive documents or digital signatures must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements

10. Network Management

1. The network of the university shall be maintained by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity
2. The network must be designed and configured to deliver high performance and reliability to meet the university's needs whilst providing a high degree of access control and a range of privilege restrictions
3. The network shall be segregated to create security zones, with routing and access controls operating between the zones, to reduce the possibility of internal or external users gaining unauthorised access to systems. Systems with particularly high-security vulnerabilities shall be protected both from internal and external access. All other systems will be protected from external access by default. Appropriately configured firewalls shall be used to protect the network supporting the university systems
4. Access to the resources on the network must be strictly controlled to prevent unauthorised access, and access control procedures must provide adequate safeguards through robust identification and authentication techniques
5. The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components. All changes must be adequately tested and authorised before moving to the live environment

6. Faculties/ departments/ units/ centres/ administrative branches should refrain from creating their own Wi-Fi networks other than for teaching and research purposes without informing the ICT Centre or the faculty ICT Centres for faculties located outside of Dalugama premises. Any access points installed should be secure and able to authenticate individual users. Ideally, these points should be connected to the secure access controller maintained at the ICT Centre/Faculty ICT Centre.

7. Moves, changes and other reconfigurations of network access points will only be carried out by authorised staff

8. The network infrastructure must be adequately configured and safeguarded against both physical attack and unauthorised intrusion

9. Remote access to resources on the network will be made available only through authorised entry points, normally through the site firewall. Remote access to non-public resources will be subject to authentication and other security mechanisms

10. Assigning IP addresses is a responsibility of the ICT Centre or the faculty ICT Centres for faculties located outside of Dalugama premises. IP addresses should only be changed by authorised staff and should not be changed without prior written notification to the ICT Centre and/or faculty ICT Centres

11. Systems Operation, Management and Development

11.1 Operations

1. The ICT Centre/Faculty ICT Centre manages, maintains and operates a range of central computing servers, systems, core network switches, backup systems, and the overall network infrastructure interconnecting these systems

2. The ICT Centre/Faculty ICT Centre shall maintain secure server room facilities with protected power arrangements and climate-controlled environments with an appropriate level of security

3. In order to provide a more secure and reliable service as well as to save resources, individual faculties, departments, centres/units and administrative branches are encouraged to utilise centralised systems to offer services such as Learning Management Systems, websites, etc. where services could be provided as centralised services

4. In order to enhance the overall security of computing systems of the university, servers that could be accessed from outside are required to be kept inside a secure server room

5. Server rooms, offices and other areas where sensitive or critical information is processed shall be given an appropriate level of physical security and access control

6. Only authorised persons will be able to access areas where sensitive or critical information is processed or critical information assets are located

7. Duties and areas of responsibility shall be segregated where practical, and based upon a risk assessment, to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the university. Where possible, this segregation of duties should be enforced by the system security

8. Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the university systems and associated services and computing and network facilities. Mechanisms shall be in place to monitor and learn from those incidents

9. Procedures shall be established for the reporting of software system malfunctions and faults in the university's computing and network facilities. Faults and malfunctions shall be logged and monitored, and timely corrective action shall be taken

10. Development and testing facilities for critical systems shall be separated from operational facilities where economically feasible, and the migration of software from development to operational status shall be subject to formal change control procedures

11. Security risks to the information assets of all system deployment and development projects shall be assessed, and access to those assets shall be controlled. This will include all aspects of integration with existing systems

12. A Disaster Recovery Plan shall be prepared, documented and tested for existing and new operational systems at an appropriate level of detail commensurate with the complexity of the system and the assessed level of criticality for the university's business. This documentation should encompass any recorded exceptions based on risks assessed and management approval given

13. Acceptance criteria for new information systems, upgrades and new versions shall be established, and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place

14. Procedures shall be established to control the development and deployment of all operational systems. All systems developed for and within the university must follow a formalised development process

11.2 Systems Management

1. The university systems shall be managed by suitably trained and qualified staff to oversee their day-to-day running and preserve security and integrity in collaboration with individual system owners. All systems management staff shall be given relevant training in information security issues

2. Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management, and any changes of access permissions must be authorised by the manager of the system or application. A record of access permissions granted must be maintained

3. Access to all information systems, except those that are publicly accessible, shall use a secure logging-on process and be limited by time of day, location of workstation, or through an automatic time-out after a defined period of inactivity, where appropriate. Access to information systems may be logged and monitored to identify potential misuse of systems or information

4. Password management procedures shall meet the requirements of the Information Security Policy

5. Systems administration or management functions shall only be performed by authorised staff. Use of such commands should be logged and monitored where appropriate

6. The implementation of new or upgraded software must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to systems. All changes must be adequately tested and authorised by the system owner before moving to the live environment

7. Capacity demands of systems supporting business processes shall be monitored, and projections of future capacity requirements made to enable adequate processing power, storage, and network capacity to be made available

8. Security event logs, operational audit logs and error logs must be adequately reviewed and managed by qualified staff

9. System clocks must be regularly synchronised by authorised staff between the university's various processing platforms

11.3 Systems Planning

1. New information systems, or upgrades to existing systems, must be authorised within the university's governance structure. The authorisation process must take account of security requirements

2. The information assets associated with any proposed new or updated systems must be identified, classified and recorded

3. Equipment supporting the university systems shall be planned to ensure that adequate processing power, storage, and network capacity are available for current and projected needs, all with appropriate resilience and fault tolerance levels. Equipment shall be correctly maintained

4. Prior to acceptance, all new or upgraded systems shall be tested and the results documented to ensure that they comply with the university's Information Security Policy, access control standards and requirements for ongoing information security management

11.4 Software Management and Development

1. Software applications are to be managed by suitably trained and qualified staff to oversee their day-to-day running and preserve security and integrity in collaboration with nominated individual application owners. All staff involved in software development and management shall be given relevant training in information security issues

2. The procurement or implementation of new or upgraded software must be carefully planned and managed, and any development for or by the university must always follow a formalised development process. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls

3. Requirements specifications for new software or enhancement of existing software shall specify the required information security controls

4. Formal change control procedures, with audit trails, shall be used for all software components of a critical system. All such changes must be risk assessed and authorised by the relevant Officer in Charge before being moved to the live environment

5. Implementation, use or modification of all software on the university systems shall be controlled. All software shall be checked before implementation to protect against malicious code

12. Business Continuity

1. The university will continue to assess business continuity requirements and to identify appropriate areas for further action

2. A formal risk assessment exercise has been conducted to classify all systems according to their level of criticality to the university and to determine where business continuity planning is needed

3. A business continuity plan will be developed for each system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates

4. All business continuity plans will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether management and staff are able to put the plan into operation

5. All relevant staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans

6. Each business continuity plan will be regularly reviewed, and if necessary, updated. The frequency of reviews will be as defined for the appropriate criticality level

13. Procurement and management of ICT related systems

1. Users are advised to use recommended specifications and guidelines to purchase general-purpose IT equipment such as desktops, laptops, printers, photocopiers, etc. During the procurement process, users are encouraged to obtain the ICT Centre's services in an advisory capacity.

2. Once equipment or systems are installed, either the ICT Centre or the respective user (in case of specialised equipment or systems) should certify that the work has been completed according to requirements

3. The ICT Centre should take ownership' of Critical ICT based systems in the university to ensure these systems are operated securely and provide a reliable service

4. In order to ensure all servers are maintained in a secure, controlled environment as well as to save resources, whereas possible individual faculties, departments, centres/units and administrative branches are encouraged to use server space provided by the ICT Centre instead of procuring new servers

14. Enforcement

Reports of problems or violations should be informed to the Director, ICT Center by emailing dictc@kln.ac.lk

Violations of policies, including the Information Security Policy, may result in appropriate disciplinary measures in accordance with the law of the country as well as regulations and policies of the university.

The ICT Centre of the university may temporarily remove or block any system, device, or person from the university network that is reasonably suspected of violating this Information Security Policy to protect the network, information technology resources and maintain business continuity.

15. Disclaimer

UoK disclaims any responsibility for and does not warrant information and materials residing on non-UoK systems or available over publicly accessible networks. Such materials do not necessarily reflect the attitudes, opinions or values of UoK, its staff or students.

Document title
Information Security Policy
Approving body
Council, University of Kelaniya
Enforcement Authority
Vice-Chancellor, University of Kelaniya
Operational responsibility
Director, Information and Communication Technology Centre, University of Kelaniya
Date of approval
10.07.2012 (394th Council)
Date (s) of approval of revision (s)
10.08.2021
Revision no.
2
Date of effect (revised version)
XX
Document classification (Public, Internal, Confidential, Secret)
Public

This policy document is authored by Dr Ruwan Wickramarachchi, Director, ICT Centre. The initial draft was reviewed by Prof B D Nanadadeva, Department of Fine Arts; Dr Janaka Wijayanayake, Department of Industrial Management; and; Mr L Jayatissa, Librarian, University of Kelaniya.