Information System administrator / Data Custodian guidelines

Contents

Introduction

Information systems administrators and members of Computing Services with elevated access rights have additional powers and access to central information systems at the University. The role of these staff within the Information Systems Security policy is defined as Data Custodians and they are responsible for the safe custody, transport, storage of the data and implementation of business rules that affect it. The University expects that staff with administrator access will exercise the highest ethical professional conduct at all times and exercise a duty of care to all users of the systems that they maintain. This document sets out the responsibilities and required behaviour of staff who maintain information systems at the University.

Scope

Information systems at the University must be managed by suitably skilled staff to ensure their continued security. These guidelines cover all staff who have elevated privileges on any University multi-user computer systems to administer the system itself or the services running on it. These guidelines also cover Service Owners who are typically team leaders who manage a team of data custodians maintaining a particular service and these roles carry additional responsibilities.

Guidelines

Data custodians are key to ensuring the security of the University's information systems. The high level requirements for Data Custodians are defined in the information Systems Security policy and form the basis for the additional guidance given here. Data custodians must:

Ensure that the physical and network security of systems is maintained.

Custodians should ensure the physical security of their servers by hosting them in the University data centres where possible or take similar or increased measures to restrict and monitor the physical access to them.

Network access to servers should be limited to only those that require access. Remote access to administrative services should be assessed separately and have additional restrictions where possible. Regular network vulnerability assessments will be made on live systems and the results published to system owners.

Ensure that the systems they maintain are suitably configured, maintained and developed.

Custodians should deploy hardened systems to agreed secure baselines based on industry practice. Baselines should be developed and documented for hypervisors, operating systems and applications. These baselines should be reviewed in response to changes in best practice.

Custodians must apply software patches in a timely manner to address published vulnerabilities or those highlighted through automatic scanning. High priority patches must be applied in accordance with supplier recommendations or within two weeks, whichever is shorter. Where this is not possible due to service commitments other compensating control measures should be taken to mitigate the risk and the risk reported to senior Computing Services management.

System times should be synchronised with a reliable time source. All information systems based on campus should sync from the University NTP servers which will in turn be synced with the official JANET NTP servers. Cloud based services should use a reliable Tier 1 source.

Changes to Information Systems should be made in line with change management processes and procedures. Changes for security measures can invoke the emergency change procedures.

Ensure that the data are appropriately stored and backed up.

System configurations should be documented and where possible held in a University version control system. System data should be backed up in all cases and to a location physically separate location where possible.

Ensure that appropriate access controls are in place to meet the requirements of Data Stewards.

Access to all systems must be made through a secure authentication process apart from read-only or publicly available information and only given to those who require access. Where possible central authentication systems such as single sign-on should be used and local accounts avoided. Administrator accounts with elevated privileges should only be used to carry out specific tasks and not used as a matter of routine. The principle of least privilege should be applied at all times.

Service owners should record the classifications of the data held on their systems and the potential access routes to this data and the controls on them. These records should be used in a discussion with the Data Stewards to ensure that they meet the levels needed.

Understand and document risks, take suitable steps to mitigate and ensure that these are understood by data owners.

Service owners should understand the deployment of information systems and the potential risks in any deployment. These should be highlighted to service owners and significant risks should be placed in the Computing Services risk register and monitored.

Document operational procedures and responsibilities of staff.

Service Owners should ensure that operational procedures are recorded and the responsibilities for staff are made clear.

Publish procedures for users of the systems to allow secure access and usage

Service Owners should ensure that sufficient documentation is made available to all users of a system to allow secure access and storage. This documentation should be reviewed and updated so that it matches current security requirements where these change in particular in relation to minimum standards for encryption.

Ensure that systems are compliant with legal and other contractual requirements

Data Custodians should ensure that they have a full understanding of the legal and contractual requirements of the data and systems that they maintain when the service is used in accordance with the service description. They are authorised to act promptly to protect the security of their systems but any actions they take should be balanced and proportionate particularly when undertaking actions that would have a direct impact on the users of their or other systems. Actions that might potentially be invasive of a user's reasonable expectations of privacy must be undertaken in accordance with the guidelines on investigation of computer use.

Logging should be put in place to record the use and attempted use of information systems. The data logged should be sufficient to support the security, compliance and capacity planning requirements. Logging for normal user actions should not be unnecessarily intrusive whereas logs for system administrator access should record all actions. Logs should be recorded on a separate system to the one being monitor and secured to prevent unauthorised modification. Logs should be held for a defined period and then deleted automatically unless they been specifically identified as required for investigation.

The Data Protection Act requires that any personal data is collected for specific purposes and is deleted when it is no longer required.

Document Control Information

Owner	Mark Acres IT Security Manager
Version Number	0.01
Approval Date	
Approved By	
Date of Last review	