Dublin City University

Asset Management Policy

Contents

Purpose

The objective of this policy is to maintain appropriate protection of organisational assets, and to avoid breaches of any criminal and civil law, statutory, regulatory or contractual obligations. This Policy provides a focus on the issues relating to the management of DCU's ICT assets.

Scope

This policy covers the following elements:

Physical Assets

End user devices:

- Desktop personal computers, laptops etc
- Other portable computing devices including PDAs and smartphones

Infrastructure:

- Servers
- Midrange/multi user systems
- Mainframes
- Storage devices e.g. Disk Arrays, Tape Libraries, etc.
- Network devices, e.g. routers, switches and hubs etc

Software Assets

Software is included where it is installed on infrastructure components and is (or may be) separately licensed. This includes, but is not limited to, Operating systems, middleware, database and application software.

Information Assets

DCU's information assets include data such as student data, employee data, financial data, and research data which are important to the University's academic and research mission.

The classification of information assets is governed by DCU's Data Classification Policy. Asset Registers will be maintained locally within the Faculty or Unit responsible for the asset.

Policies and management

All assets have a defined asset custodian. The custodian has overall responsibility for the integrity, availability and protection of the asset. DCU retains overall responsibility and ownership for all assets, but individuals, schools and units etc are tasked, as custodians, with creating and maintaining these assets. Custodians of ICT assets are responsible for the protection, integrity and availability of those assets and for putting the appropriate controls and procedures in place.

Asset Life Cycle

Asset Acquisition

- Assets covered under the scope above must be sourced via a DCU approved supplier.
- University policy and local procurement guidelines must be followed. ICT acquisitions requiring the support of ISS must be agreed with ISS prior to procurement.
- All purchase of new systems hardware / software or new components must be made in accordance with relevant Information Security and other University policies, as well as technical standards.

Installation

- All authorised equipment must be fully and comprehensively evaluated, tested, assessed for fitness of purpose, hardened to security standards and formally accepted by the users before being transferred to the live environment.
- Hardening standards must be followed for all new hardware and software prior to production implementation.

Disposals and Recycling

- All data and configuration setting (including User Ids and passwords) must be permanently deleted prior to disposal.
- Computer Equipment must be disposed of in a safe and environmentally friendly manner, in accordance with local legal requirements (including copyright principles and licence terms)

Rights of Use – Software Licensing

- Approval of software licence agreements (Including EULAs,/End User Licence Agreements) must only be done through approved processes.
- Purchasing documentation (including executed contracts) relating to software must be filed and retained in perpetuity to provide a historical record and evidence of prior licensing arrangements, including evidence of entitlement to current versions of software based on an upgrade path.
- Software licence certificates must be retained in a secure environment with limited and managed access controls.

Outsourcing and Third Parties

- Controls must be in place to ensure that the third party outsourcer complies with University asset management policies.
- Controls must be in place to ensure that third parties, outsourcers and service providers do not put DCU at risk by not providing sufficient licence rights for software used by DCU staff.
- Controls must be in place to ensure that third parties, outsourcers and service providers comply with the restrictions and requirements set out in DCU's licence agreements where applicable.
- On termination of an outsourcing or services agreement, DCU must provide for sufficient licence rights to continue using computer software previously provided by the outsourcer.
- Controls and reporting processes must be in place to verify the efficient use of assets employed in the delivery of services to DCU to ensure that DCU's investment is maximised.

Asset Register

- All assets covered under the scope above (owned and leased), excluding end user devices, must be captured on the appropriate Security Asset Register.
- All such assets must have an identified custodian, captured in the asset register, and be tracked throughout its lifecycle.
- Periodic checks of the hardware and software installed may take place to ensure that the asset register is an accurate reflection of the physical installations.
- Assets owned by the University may only be disposed of with the agreement of the assigned IT Asset custodian.

- When such assets are disposed of, the Security Asset Register must be updated to show that IT equipment / hardware has been decommissioned and the method of its disposal (the asset must not simply be deleted from the register).

Disaster and Business Recovery

Custodians must be able to demonstrate that critical business applications that include licensed software are identified and that the licence permits use of that software at a different site, university location or computer all of which may be operated by a third party.

Document Change Management

Dublin City University believes that it is important to keep this Asset Management Policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed

The Director of Information Systems and Services (ISS) will draft necessary changes and have them reviewed and approved by the Executive Group of DCU as appropriate. The Director of ISS and the members of the ICT Security Implementation Group will communicate changes to the University communities. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this policy should be communicated to the Director of ISS.