Proposed IT Services Records Retention Schedule.

General Classes of Records Held:	Default Retention Period – This is the suggested time period for which these records should be held based on legal precedence and experience elsewhere:	Rationale:	Final Disposition: After the retention period expires the records should be archived or shredded:	Record Owned/Managed By:
IT strategy.	Retain until superseded plus a minimum 5 years.	To facilitate continuity in strategy development.	Archive one copy and destroy remainder by confidential shredding/ secure deletion.	CIIO.
Operational policies & procedures.	Retain until superseded plus a minimum 5 years.	No longer needed after this point.	Archive one copy and destroy remainder by confidential shredding/ secure deletion.	Director of IT Services.
IT governance, agenda, minutes, project submissions.	Retain permanently.	Part of University record.	Archive.	Secretary of IT Management Steering Committee (ITMSC).
Records documenting the management of IT systems development projects.	Retain until end of project plus a minimum of 5 years.		Destroy by confidential shredding/ secure deletion.	Director of IT Services.
IT risk register.	Retain permanently in current form.	To facilitate risk management.		Director of IT Services.
Reports of major IT incidents.	Retain for duration of incidence, review period and until any recommendations therein are carried out plus a minimum of 5 years.	To facilitate the generation of resilient services and support planning and strategy development	Archive one copy and destroy remainder by confidential shredding/ secure deletion.	Director of IT Services.
Plans for recovery in the event of a major IT incident.	Retain permanently in current form.			Director of IT Services.

Maynooth University
National University of Ireland Maynooth

General Classes of Records Held:	Default Retention Period – This is the suggested time period for which these records should be held based on legal precedence and experience elsewhere:	Rationale:	Final Disposition: After the retention period expires the records should be archived or shredded:	Record Owned/Managed By:
Change management records documenting initial development and post implementation modification and maintenance of IT systems.	Retain until proposed system is decommissioned plus a minimum of 5 years. For systems not implemented retain for a minimum of 5 years from the date of the last action taken on the development.	To facilitate change management.	Destroy by confidential shredding/ secure deletion.	Director of IT Services.
Records documenting security arrangements for IT Systems.	Retain until decommissioning of relevant system plus a minimum of 5 years.	To facilitate the transition from old to new systems.	Archive one copy and destroy remainder by confidential shredding/ secure deletion.	Director of IT Services.
Records documenting security incidents involving MU IT systems.	Retain for a minimum of 6 years from last action on the breach.	To facilitate a civil claim in Tort or Contract Law if relevant.	Archive one copy and destroy remainder by confidential shredding/ secure deletion.	Director of IT Services.
Records documenting the routine monitoring and testing of the operation of IT systems, and actions taken to rectify problems and optimise performance.	Retain for current year plus a minimum of 1 year.	Good practice: To facilitate ongoing maintenance and optimisation of IT systems.	Destroy by confidential shredding/ secure deletion.	Director of IT Services.
Records documenting the management of system data storage, including the operation of data backup, archiving and deletion routines.	Retain for current year plus a minimum of 1 year.	Good practice: to facilitate oversight and optimisation of the process.	Destroy by confidential shredding/ secure deletion.	Director of IT Services.

General Classes of Records Held:	Default Retention Period – This is the suggested time period for which these records should be held based on legal precedence and experience elsewhere:	Rationale:	Final Disposition: After the retention period expires the records should be archived or shredded:	Record Owned/Managed By:
Records documenting user requests to recover data from backup or archive stores and action taken	Retain for minimum of 1 year from last action on request.	No longer needed after this point.	Destroy by confidential shredding/ secure deletion.	Director of IT Services.
Records documenting the arrangements for the sanitisation of institutional IT equipment prior to disposal.	Retain for a minimum of 1 year from disposal of equipment.	No longer needed after this point.	Destroy by confidential shredding/ secure deletion.	Director of IT Services.
Records documenting the maintenance of appropriate software licences for live IT systems.	Retain until superseded.	No longer needed after this point.	Destroy by confidential shredding/ secure deletion.	Director of IT Services.
Records recording the request for, creation, maintenance and closure of user accounts for IT systems.	Retain for a minimum of 1 year from closure of account.		Destroy by confidential shredding/ secure deletion.	Director of IT Services.
Records documenting user requests for technical and application support and action taken to investigate and resolve the problem.	Retain client details for duration of formal association with University.		Delete any personal details e.g. private contact details, from ticketing system.	Director of IT Services.

General Classes of Records Held:	Default Retention Period – This is the suggested time period for which these records should be held based on legal precedence and experience elsewhere:	Rationale:	Final Disposition: After the retention period expires the records should be archived or shredded:	Record Owned/Managed By:
Requests for and authorisation of connections of third party equipment to the MU network, either on premises or via dial-up communications links.	Retain for a minimum of 1 year from termination of connection.	No longer needed after this point.	Destroy by confidential shredding/ secure deletion.	Director of IT Services.
Records of mobile IT equipment held off-site.	Retain until return of equipment.	No longer needed after this point.	Destroy by confidential shredding/ secure deletion.	Head of relevant department/ school/ unit.
OpenLDAP: The legacy directory service that is in the process of being replaced by Active Directory holds basic account data (username, names, email addresses, phone numbers & staff/student numbers). There are also logs of which user authenticated to which service from which IP, when.	Indefinitely. Logs are written to disk on the servers, and the servers are backed up, so the logs will remain present as long as the backups are retained.	Required for the operation of the service.		IT Services

General Classes of Records Held:	Default Retention Period – This is the suggested time period for which these records should be held based on legal precedence and experience elsewhere:	Rationale:	Final Disposition: After the retention period expires the records should be archived or shredded:	Record Owned/Managed By:
Active Directory: The university's directory service holds basic account information (usernames, names, email addresses, phone numbers & staff/student numbers. There are also logs of which user authenticated to which service from which IP when.	Indefinitely Logs are backed up along with the Windows VMs themselves, so retention of the logs depends on retention of the server backups.	Required for the operation of the service.		IT Services
Server Log Aggregator (syslog): The centralised logging server logs events that contain usernames, IP addresses & MAC addresses for some servers. (Scope is servers with Linux OS and some applications.)	6 months	Auditing, error detection, investigation of incidents.		IT Services.
DDI Systems (DNS, DHCP & IPAddress Management): these systems contain information that could be used to indirectly identify people including IP address allocations and MAC addresses. The DHCP logs map MAC addresses to IP addresses at given times.	Indefinitely	Required for the operation of the system.		IT Services

General Classes of Records Held:	Default Retention Period – This is the suggested time period for which these records should be held based on legal precedence and experience elsewhere:	Rationale:	Final Disposition: After the retention period expires the records should be archived or shredded:	Record Owned/Managed By:
Office 365: Microsoft's cloud services provides email, file storage, groupware, and collaboration tools to university staff and students. To facilitate the provision of these services a copy of much of the data in our on-premise AD is synchronised with Microsoft's Azure AD cloud service. This includes names and email addresses.	Max 180 days according to Microsoft's Data Handling Standard policy for Office 365 at https://docs.microsoft.com/en-us/office365/enterprise/office-365-data-retention-deletion-and-destruction-overview	Required for the operation of the system.		IT Services & Microsoft
Network Security Systems: Logs of access by username to the Internet. Security Director software is used to parse logs from campus perimeter firewall.		Required for the operation of the system, investigation of security and service incidents.		IT Services

General Classes of Records Held:	Default Retention Period – This is the suggested time period for which these records should be held based on legal precedence and experience elsewhere:	Rationale:	Final Disposition: After the retention period expires the records should be archived or shredded:	Record Owned/Managed By:
Network Management Systems: the systems for managing the university's wired and wireless networks log information that could be used to indirectly identify people including IP addresses & MAC addresses. The wireless logs include user/device match to nearest access point.	Indefinitely	Required for the operation of the system, investigation of security and service incidents.		IT Services
Campus Telephone System: names of users of campus telephones		Telephone System Administration		IT Services

End of IT Services Records Retention Schedule.