I. Policy Statement

Specific types of institutional data entrusted to the University shall not reside within any cloud computing environment unless UMass Lowell has entered into a legally binding agreement with the service provider, reviewed and approved by Purchasing, Information Technology, and/or the Office of General.

Additionally, personal cloud services accounts are prohibited for the storage, management, or sharing of University institutional data. Any University data residing within a cloud computing environment must be retrievable by the institution and not solely by the individual who placed the data in the cloud environment.

II. Purpose

The purpose of this policy is to ensure that UMass Lowell institutional data is not inappropriately stored or shared using public cloud computing and/or file sharing services. Cloud computing and file sharing, for this purpose, is defined as the utilization of servers, storage, or information technology hosting of any type that is not controlled by, or associated with, UMass Lowell.

III. Scope

This policy applies to all UMass Lowell employees and extends to cloud computing resources that provide services, platforms, and infrastructure that provide support for processing, exchange, storage, or management of institutional data.

IV. Definitions

Cloud Computing – in the context of this policy, encompasses utilizing any external computing, software services, or hosting environment that is not directly controlled by, or associated with, UMass Lowell.

Institutional Data – Information entrusted to the University for the purpose of conducting official business. Can be classified as either Restricted, Confidential, Operational or Unclassified.

Encrypted data - refers to information that has been converted through software into a non-human readable form typically via a password or phrase (which is also used to decrypt the file when the information is to be accessed). All encryption referred to within this policy should conform to prevailing industry standards.
Restricted Data – Very High Sensitivity: Information legally classified as breach notifiable and where UMass is required to self-report to the government and/or provide notice to the individual if the information is inappropriately accessed. Examples include, but not limited to: social security numbers, credit card numbers, Passport ID Numbers and Other forms of Official Government Issued Identification; bank account numbers, Export Controlled data, medical records.

Confidential Data – High Sensitivity: Any information that is contractually protected as confidential by law or by contract and any other information that is considered by the University appropriate for confidential treatment. Such data should not be copied or removed from UMass Lowell operational control without authorized permission. High sensitivity data is subject to restricted distribution and must be protected at all times. Compromise of high sensitivity data could damage the mission, safety or integrity of UMass Lowell, its staff or its constituents. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law. Examples include, but not limited to: student educational records, students or parents’ financial records, names in combination with driver’s license numbers or stated ID card numbers; student and employee IDs.

Operational Use Only Data – Medium/Moderate Sensitivity: any information that is proprietary or produced only for use by members of the University community who have a legitimate purpose to access such data. Release of this data must be approved prior to the dissemination out UMass Lowell. Its compromise may inconvenience a department, but it unlikely to result in breach of confidentiality, loss of value, or serious damage to integrity. This information is critical to the University’s academic, research, and business operations that require a higher degree of handling than unclassified (public) data. Examples include, but not limited to: system configuration/log files, staff meeting notes, business process documentation, campus infrastructure plans.

Unclassified (Public) Data – Low Sensitivity: any information that may or must be made available to the general public, with no legal restrictions on its access or use. Security at this level is the minimum required by UMass Lowell to protect the integrity and availability of this data. Examples include, but not limited to: student directory information (unless restricted), campus maps, class schedules, course catalogs, policies and procedures.

V. Procedures

Departments considering the use of third-party cloud computing services, platforms, and infrastructure that provide support for processing, exchange, storage, or management of institutional data, must first consult with Information Technology to identify the data classification type, business use, and information security requirements. Send email to infosec@uml.edu for more information regarding the types of data that can be stored in the cloud.

A. Restricted and Confidential Data

Departments are required to consult with Purchasing, Information Security, and/or the Office of General Counsel to ensure that the data is protected and managed in accordance with policies, procedures and standards required by law and acceptable to the University.
B. Operational and Unclassified (Public) Data

It is recommended that departments consult with Purchasing and Information Security to ensure that the data is protected and managed in accordance with policies, procedures and standards required by law and acceptable to the University.

VI. Responsibility

Information Technology is the responsible organization for implementing the provisions of this policy. The University’s Chief Information Officer and the Information Security Officer are the designated point of contacts.

VII. Attachments

N/A

VIII. Related Policies, Procedures and Announcements

UMass Lowell Data Classification Policy
University of Massachusetts Procurement Policy

<table>
<thead>
<tr>
<th>Effective As Of:</th>
<th>October 4, 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Review Date:</td>
<td>October 4, 2018</td>
</tr>
</tbody>
</table>