University of Portland

CLOUD APPLICATION AND INFRASTRUCTURE POLICY

1. **PURPOSE:** This policy outlines best practices and approval procedures for procurement and use of cloud computing services for the processing, sharing, storage, and management of institutional data at the University of Portland. This policy is meant to ensure that cloud services are NOT purchased or used without the knowledge of an Information Services (IS) Director or CIO. University of Portland data is not inappropriately stored or shared using public cloud software or infrastructure.

2. **SCOPE:** Cloud computing is defined as the utilization of information technology hosting of any type that is not controlled by, or associated with, University of Portland for services such as, but not limited to, web applications (e.g., social media, blogs and wikis), file storage, content hosting (e.g., publishers text book add-ons) or enterprise applications (i.e., Software-as-a-Service). This policy applies to all cloud computing resources at the University of Portland. Other University policies are referenced that may apply to the handling of specific information in specific instances. When a more specific policy applies, it should be followed.

3. **POLICY:** It is imperative that employees NOT open cloud service accounts or enter cloud service contracts for the storage, manipulation or exchange of university-related communications or university-owned data without an IS Director or CIO's input. This is necessary to protect the integrity, security and confidentiality of university data and the security of the university's network. When University data is processed or stored in Cloud products it is always subject to University security policies. Please reference the *Data Risk Classification Guidelines* listed on the Information Services website. These guidelines define Level 1 (High Risk), Level 2 (Moderate Risk) and Level 3 (Low Risk) data sets and outline approved technologies for each level.

   a. User access and authentication must be controlled consistent with University identity and access management policies.

   b. Use of cloud services for storage, communication and productivity involving University Level 1 data is prohibited

   c. Use of cloud services for storage of University Level 2 data is limited to services approved, contracted by or supported by the University's Information Services division.

   d. Use of cloud service offerings which are not approved, supported, provisioned or contracted by the University's Information Services division for storage, communication, and productivity are prohibited. This applies to any use of University records including vital records which are classified as public or Level 3 data. University data access should be limited to University supported, provisioned and contracted services only.

   e. The use of public cloud services for academic, non-FERPA, non-HIPAA data is permitted.

   f. Use of cloud computing services for business needs must be formally authorized by an IS Director or the CIO. The CIO will direct the IS security team to conduct a Data Risk Assessment (DRA) which will certify the cloud vendor meets all university security, privacy and policy requirements. Guidance on how to proceed will be provided based on the DRA. This could include, but is not limited to amending contracts, removing data fields we share with the vendor or requiring external audit results of the vendor.

   g. All cloud applications and services must meet University accessibility standards.

h. For any cloud services that require users to agree to terms of service, such agreements must be reviewed by an IS Director, CIO or the VP for University Operations. The use of such services must comply with the University of Portland's Acceptable Use Policy and with all laws and regulations governing the privacy and handling of personally identifiable information, financial data or any other data owned or collected by the University of Portland.

i. Data in the cloud must comply with the University Information Security Policy.

j. Personal cloud services accounts may not be used for the storage, manipulation or exchange of University information in the form of communications or data.

4. GUIDANCE: The following guidelines are intended to help the University of Portland community review, choose, and purchase the best cloud solution for their needs and to establish a process whereby University of Portland employees can use cloud services without jeopardizing university data and computing resources. Information Services Directors and the CIO are available to collaborate with you through this process.

a. **Procurement and Approval Process:** To start the cloud services procurement and approval process, submit an online *Technology Project Consultation Request* via the Tech Support Portal at support.up.edu. Upon receipt, IS staff will guide you through the following steps:

- Technical Consultation
- Contract Review
- Data Risk Assessment (DRA)
- Security Review (via the HECVAT)
- Accessibility Review (via the VPAT)
- Pricing Negotiations
- Order and Payment Processing
- Project scheduling and planning for any IS related efforts for implementation or integration

b. **Researching a Cloud Solution:** Does your group want to move its servers, applications, or other IT resources to the cloud, or investigate a cloud solution to meet a business need? There are many technical and business issues to consider when choosing a cloud solution. The detailed information in the sections below will help you to determine the best fit for your needs.

- **Review Criteria for Cloud Solutions:** The best cloud solutions for the University of Portland will:
  - Meet your business requirements.
  - Integrate with your infrastructure and authentication.
  - Meet University of Portland information security requirements.
  - Fit your portfolio as it changes over time.
  - Be produced by a viable company with a strong track record.
  - Align with the staff expertise that will be available to you.

- **Security Considerations:**

General Security Considerations

Considerations	Questions to ask	Reference
Support of security standards	Is the potential Cloud vendor compliant with relevant security standards?	Information Security Policy
Notification of breaches	What is the Cloud vendor's policy regarding notifying customers of security breaches? Will you get adequate notification from the vendor to fulfill University obligations as described in the Information Security Policy	Incident Response Plan
Identity and access management	Does the solution provide support for the University's identity and access management (IAM) requirements? Objective is for University of Portland users to use their SSO credentials to securely access the vendor's application or resource. What types/levels of user security, authentication and authorization options are available (e.g., SAML, LDAP, MFA, other)?	Authentication and Access Policy

Data Security Considerations

Considerations	Questions to ask	Reference
Data Ownership	Confirm that the University owns its data under all circumstances, including the raw data supplied by the University and the results of processing on the provider's cloud platform or application. Ensure that the vendor is obligated to return all data under any possible termination scenario and destroy any remaining copies.	Data Standards for the University of Portland
Location of data	Where will the data physically reside? Who is the hosting provider and where is the data located? What type of infrastructure is the data stored on? Does the data cross international borders?	Information Security Policy
Protection of Data	Is the data being processed or held Level 1, Level 2, or Level 3 risk data? Will HIPAA, PHI, FERPA, or other protected data ever be in the system? Does the solution comply with PCI-DSS if processing credit card data?	Data Risk Classification Guidelines
Deletion of Data	Confirm that the University maintains the right to sanitize (destroy) its data at any time.	Vendor Management

		Policy

- **Choose a Cloud Solution Type**

  - **Software-as-a-Service (SaaS) – Generally preferred**
    Software-as-a-Service (SaaS) is managed and hosted by the vendor and accessed through your browser. Because the vendor maintains everything needed to run SaaS, including the software, servers, and storage, SaaS requires less technical expertise than other cloud solutions. It is a popular cloud solution choice at the University of Portland, where SaaS products have been deployed for over a decade. Popular SaaS products include Microsoft Office 365, Slack, ServiceNow, Dropbox, and Amazon Web Services. Software-as-a-Service is the University of Portland's recommended choice if it meets your needs and is approved.

  - **Platform-as-a-Service (PaaS) – If SaaS doesn't meet your needs**
    With Platform-as-a-Service (PaaS), the vendor manages the software platform infrastructure, and you develop, run, and manage applications and data on that platform. PaaS requires the technical expertise to develop and operate applications on a cloud platform. Popular PaaS products include Microsoft Azure, AWS Elastic Beanstalk, and Force.com by Salesforce. IS does not generally recommend PaaS for departments to manage and maintain. PaaS products usually fall under IS management and it's critical that departments work with IS leadership to find resources to support the service

  - **Infrastructure-as-a-Service (IaaS) – If PaaS doesn't' meet your needs**
    With Infrastructure-as-a-Service (IaaS), you create an infrastructure in the cloud using resources provided by an IaaS vendor, then you develop, run, or manage software within that system. IaaS is the most customizable cloud solution, but it also requires the technical expertise to create and manage an infrastructure and to develop and/or operate software in the cloud. Popular IaaS vendors include Google Cloud Platform, Microsoft Azure, and Amazon Web Services. IS does not generally recommend IaaS for departments to manage and maintain. PaaS products usually fall under IS management and it's critical that departments work with IS leadership to find resources to support the service

- **Purchase a Cloud Solution:** University of Portland Information Services has contracts and agreements with a variety of vendors. For a list of these vendors, see our *Data Risk Classifications Guidelines*. You are strongly encouraged to take advantage of existing cloud services and established vendors. If a new product is required, it must be carefully vetted via the Information Services technology security review process. A DRA must be issued to proceed to purchase. By working in concert with Information Services on all purchases of cloud services, the University can avoid duplication, achieve best pricing and contract terms, as well as ensure a technically sound solution that addresses data integration needs and meets all security requirements.

5. **EXCEPTIONS:** When no protected data sets are involved (i.e. no FERPA, PII, PCI, HIPPA data), the use of public cloud services for academic purposes is permitted. There are no other exceptions.

6. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.