ADMINISTRATIVE PROCEDURES

SECTION: 600 – Information Technology		**POLICY#:** 606-A
TITLE: Cloud Service Procedure		**R & O #:** 23-58
SPONSORING DEPT/DIV: Department of Information Technology Services (ITS)		**SPONSORING DEPT/DIV:** Department of Information Technology Services

OBJECTIVE: To establish procedures and guidelines for the review and technical risk assessment of all Cloud services before procuring and/or use, with the objective to maximize the value of applications, assure information security, and to set requirements based on standards for how the County handles all information assets.

DEFINITIONS

Cloud Service Provider (CSP) - A company or entity providing the cloud service, usually in a subscription model.

County Solution Sponsor (CSS) - A department or division representative (any individual requesting the solution) who will sponsor the cloud-hosted solution.

Protected Data - Protected information, also called sensitive information or County Protected Data, refers to data, personal details and other information that is protected under the law. It includes:

a) Credit card data,
b) Personal information, such as social security numbers,
c) Electronic protected health information, such as medical records,
d) Federal taxpayer information,
e) Information about employees, such as personnel records,
f) Criminal justice information, such as law enforcement data,
g) Other sensitive information related to County business, if breached could have negative repercussions to the County's reputation.

Technical Risk Assessment - The process of analyzing a CSP and assigning a risk rating reflecting the CSP's security maturity. Factors considered in a risk rating; environmental factors such as patching, network filtering and email security and whether the CSP had a recent breach event.

Full Technology Risk Assessment - This assessment is more comprehensive than a standard Technical Risk assessment because the cloud solution:

a) Will interact with County protected data,
b) Has infrastructure that will connect to the County network, or
c) Is responsible for a county critical platform or process.

Annual Cloud Risk Report - A report for IT Services (ITS) Department Leadership and Cloud Solution Sponsors to show the level of cloud service risk to the County and the County's constituents. If a CSP or the County's cloud service portfolio goes beyond the County's defined risk threshold, then the County CSS stakeholders will actively remediate the risk to bring the rating back to the County's acceptable risk threshold.

Ad hoc County CSP Audits - An ad hoc audit performed by ITS in partnership with CSS' to verify CSP services still meet County security requirements and to remove services no longer in use. If the CSP does not meet security requirements at the time of the audit, ITS and CSS will work with the CSP to remediate vulnerabilities to meet County security requirements or discuss the possibility of contract termination.

Technical Risk Assessment Procedures and Guidelines:

1. Requests to use a CSP must be submitted to ITS using the Service Portal and by completing a Cloud Service Review Request.
    a. This requirement applies whether the Cloud Services provider charges fees for the service or not.
    b. This requirement also applies for vendor demonstrations (demos).
2. Prior to submitting a request, departments should review the list of approved cloud services published on ITS' Service Portal.
    a. If a CSS chooses to use a previously approved cloud service, the CSS should notify the ITS Security Division to certify that the new business use case aligns with the initial approval and to update ITS' asset inventory tracking system.
3. Upon receipt of the request, ITS will perform a Technical Risk Assessment.
    a. If the cloud service is determined to require a Full Technical Risk Assessment review, ITS will send the CSP:
        i. The Technical Risk Assessment findings for the CSP to mitigate any security issues identified.
        ii. The Cloud Services Provider form with a request for artifacts to assist in the assessment of the service. *If a non-disclosure agreement (NDA) is required, the CSS will be responsible for its execution.

4. ITS will conduct a Technical Risk Assessment of the cloud service with the objective of mitigating discovered technology risks to an acceptable risk level for County business use.
    a. It is the CSS' responsibility to ensure that the CSP responds and mitigates identified cyber security issues in a timely manner.
        i. CSS acknowledges the cyber security issues highlighted in the Technical Risk Assessment review and works with ITS and CSP to verify all cyber security issues pertaining to the cloud service use case has been mitigated.
5. ITS will notify the CSS of cloud service and other necessary parties of approval/denial in the work request within the ITS asset tracking solution. If approved, ITS will:
    a. Append the CS Security Compliance Acknowledgement form to the work request. This form documents CSS actions and contract language required to manage the risk of using of the service.
    b. Create a Knowledge Article (KB) to be available on the ServiceIT work request portal as a reference for departments seeking cloud solutions. The KB provide the summary of service and type of data stored.
    c. Notify Risk Management and Purchasing of cloud service approval with a copy of the CS Security Compliance Acknowledgement form to inform the contracting process.
6. CSS has the right to appeal ITS' denial as described under Procedure 605-B Appeal Process for Technology Denials.

Cloud Solution Sponsor (CSS) Roles and Responsibilities:

1. The CSS is solely responsible for managing the use and risk of the CSP subscription.
2. The CSS is solely responsible for ensuring the Technical Risk Assessment recommendations and requirements are included in the fully executed contract documents.
3. Account Management - ensure the user accounts meet the ITS Identification and Authentication Policy and the respective regulatory information security requirements (e.g., HIPAA, CJIS, etc.).
4. Data Security - access controls must be managed by the CSS. The CSP does not typically manage access controls.
5. ADFS/Single Sign On (SSO) - as a security best practice, business units are strongly encouraged to use this feature or Multifactor Authentication.
6. Monitoring and Detection - CSS should monitor access logs on a weekly basis to ensure none of the County accounts on the CSP platform have been compromised.
7. Incident Response Plan – If County protected data is stored in the cloud solution, CSS must develop a business incident response plan if CSP was compromised, or a data breach occurs. This is a requirement for Oregon Consumer Information Protection Act and other regulatory security compliance requirements.

8. Retention and Public Records - any County information stored in the cloud is subject to retention in accordance with Oregon Public Records Law. The CSS is responsible for ensuring that this information is retained and available for the amount of time as prescribed by law. If the CSS does not know the retention rules, County Counsel or the County Archivist can provide support.
9. County Data Backup - CSS is responsible for data backups either through agreement with CSP or by implementing a process to periodically download data. If the CSP suffers an outage where stored data is compromised, County data must be restored in the CSP platform.
10. Data Portability - upon termination of a subscription agreement, the CSS is responsible for either that the agreement addresses CSP's assistance with migrating County data or the CSS must move the data manually. In either case, the CSS should plan to ensure that they are not expending additional supplemental subscription costs for additional time to move the data.
11. Right to Audit - this clause needs to be included in every CSP agreement as an amendment. Contact County Counsel for the exact language. This is required due to the ongoing regulatory security compliance assessments and audits performed by the ITS Security Division and the Auditor's Office.

ITS' ON-GOING RISK MANAGEMENT

1. ITS will maintain a registry of all approved cloud services used for County business.
2. ITS will maintain a system to track cyber security alerts on all cloud services that underwent a Technical Risk Assessment.
3. ITS will work with the CSS to immediately remedy cyber security alerts that indicate:
    a. A provider's risk rating falls below the County risk tolerance.
        i. CSP risk rating threshold is 7 and above.
    b. An incident, critical vulnerability or data breach has been reported on a CSP solution that collects sensitive data.
4. Develop the Annual County Cloud Risk Report to hand off to County leadership for review.
5. Perform Ad hoc County CSP Audits

(rev. February 2024)