Security Safeguards for Stand-Alone Cloud Applications

Summary:
When choosing the best way of protecting information stored in the cloud, keep in mind how valuable that information is to UNM and what safeguards are needed to reasonably protect the data. The first thing you should do is define the level of privacy needed, and thus a level of protection or safeguards.

If you use cloud storage to store university records you'll find paying for safe and secure data storage reasonable. Try to strike that delicate balance between the required level of protection and reasonably expected time/effort/money spent to implement safeguards.

HSC IT Security Requirements:
Departments requesting to purchase a cloud application (stand-alone accounts) must define the records to be stored in the cloud and the value/sensitive of those records. The department must maintain written policy and procedures that document reasonably expected safeguard for protecting the cloud stored data. HSC IT security will review the department’s policy and procedures against the guidance listed below. IT Security may recommend changes to local department policy and procedures before notifying UNM Purchasing that an IT security review has been successfully completed.

The level of detail expected in departmental application policy and procedures should address business requirements and provide for reasonably expected safeguards that match the level of risk. Many consumer type applications, that contain minimal sensitive information, can be approved with a brief written department policy and procedures (one page).

Policy Recommendations:
1. Define the Information Stored in the Application
   Include in the policy a description of records that are allowed and not allowed in the application, i.e., Protected Health Information, SSN, or other confidential information.

2. Implement Strong Authentication Protocol
   The traditional username/password combination may be insufficient to protect user accounts from hackers. Define password complexity requirement including the requirement that the password must be unique (different than the HSC NetID password). If available, use two-factor or multi-factor authentication for logging into all your cloud applications to ensure that only authorized personnel can access the data.

3. User Access Management Solutions
   Most employees don't need access to every application, every piece of information, or every file. Define proper levels of authorization to ensure that each employee can only view or manipulate the applications or data necessary for them to do their job. Define how to assign user access rights to prevent an employee from accidentally editing information that they aren't authorized to access, but also protects your systems from hackers who have stolen an employee's credentials.

   Require that accounts holders registers the account using an official HSC email address for password resets and other notifications.

4. Monitor, Log, and Analyze User Activities

HSC Information Security Office Guidance
Date: 2/12/2019
Security Safeguards for Stand-Alone Cloud Applications

Define how the application will be monitored to analysis user activities and spot irregularities that deviate from normal usage patterns, e.g., log in from previously unknown IP or devices. These abnormal activities could indicate a breach in your system so catching them early on can stop hackers in their tracks and allow you to fix security issues.

5. **Create a Comprehensive "Offboarding" Process**

Create procedures when employees leave the department they can no longer access systems, data, customer information, and intellectual property. Since each employee would likely have access to many different cloud applications and platforms, you need a systemized de-provisioning process to ensure that all the access rights for each departing employee are revoked.

6. **Provide Employee Training**

Hackers can gain access to secure information by stealing employees' login credentials through social engineering techniques such as phishing, spoof websites, and social media spying. Define minimum training on cybersecurity to prevent employees from falling victim to scams and compromising your company's sensitive data.

   Establish training and procedure to ensure that practices for protecting credentials and data during transmission using encryption are verified and followed (look for the “S” on “HTTPS” websites).

7. **Implement a Data Backup and Recovery Policy**

The average cost of IT downtime can be significant to the department, so it's important to minimize the impact of a cybersecurity breach on your organization. Devise a comprehensive data backup and recovery solution to protect all your information and make sure business-critical data can be retrieved with as little disruption as possible in the event of a security breach.

   The department policy should defined an exit strategy for retrieving the department’s data at the end of the vendor contract.