Secure Cloud Usage Guideline

Purpose

This secure cloud usage policy is meant to inform and educate end users on how to securely use cloud services.

Cornwall-Lebanon School District's IT department is committed to securing the organization's IT systems and data while enabling employees to carry out their jobs as efficiently as possible through the use of different technologies. The following policy and guidelines outline how end users can use cloud services in a secure manner without compromising Cornwall-Lebanon School District's data, IT systems, or ability to conduct business.

Scope

This Secure Cloud Usage Guideline applies to all business processes and data, information systems and components, personnel and physical areas of Cornwall-Lebanon School District.
These guidelines include all cloud services being used by Cornwall-Lebanon School District. This includes all cloud-based email, document storage, Software as a Service, Platform as a Service, Infrastructure as a Service, etc. Employee personal cloud accounts are excluded.

Cornwall-Lebanon School District currently uses Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

- Software as a Service (SaaS). A SaaS model is a software delivery and licensing model in which the software is centrally hosted by a service provider and is licensed on a subscription basis. This policy applies to all instances of SaaS that Cornwall-Lebanon School District currently uses.
- Platform as a Service (PaaS). A PaaS model is a cloud delivery model in which a platform for customers to develop, run, and manage web applications is provided on a subscription basis. This policy applies to all instances of PaaS that Cornwall-Lebanon School District currently uses.
- Infrastructure as a Service (IaaS). An IaaS model is a computing infrastructure delivery model where virtualized computing resources are provided over the Internet on a subscription basis. This policy applies to all instances of IaaS that Cornwall-Lebanon School District currently uses.

Guidelines

Data Classifications and Restrictions

All data moving to and through Cornwall-Lebanon School District's usage of cloud services is subject to and must adhere to organizational defined data classification levels.

Regulated Data

- If at any point the flow of data will contain personally identifiable information (PII), credit card numbers, data covered under HIPAA, confidential corporate data or any other sensitive or regulated data, the data should be encrypted before being moved to a cloud environment.
- Any usage of cloud services must adhere to all applicable laws and regulations governing Cornwall-Lebanon School District.

Identity and Access Management

- Prior to being granted access to an information system, each user must be provided with formal authorization by an appropriate official (i.e. the owner of the information system, the custodian of the data housed within the information system, or a designee of these individuals). This authorization will be based on definitive and verifiable identification of the user and will be logged by the authorizing official.

- Once authorization has been granted, the user will be provided with a unique information system identifier. Examples of identifiers include user IDs and employee numbers.
- Additionally, the user will be provided with a unique information system authenticator that is tied to the assigned identifier. Examples of authenticators include passwords and tokens.
- Identifiers and authenticators will be delivered to the authorized user in such a manner as to ensure they are received only by the authorized user. To minimize risk, identifiers and authenticators for critical information systems will not be provided together.

For any end users accessing cloud services, a minimum level of authentication and authorization must be met. This includes:

- Single Username and Password
  - Passwords must be constructed according to set length and complexity requirements. As such, passwords must be eight characters in length and must include upper and lower case letters, numbers, and special characters.
  - Passwords will have maximum lifespan. As such, passwords must be replaced at a maximum of 45 days.
  - Passwords may not be reused any more frequently than every five password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
  - Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically except in Corporate-authorized systems.
  - Employees must not share log-in credentials with co-workers.

Acceptable Devices and Locations

Any end users accessing cloud services may do so from a pre-approved list of mobile devices based on compatibility and configuration with our own security controls and to maximize cloud service provider owned security controls.

End users may connect to cloud-based services either from the Cornwall-Lebanon School District network or a private secure network.

When connecting from private personal networks or public networks, secured connections and transmissions must be used.

Cloud Procurement Guidelines

Any end users, working groups, or departments looking to use some cloud services for either single project based work or ongoing work, must follow these guidelines:

- The use of cloud services must adhere to existing Cornwall-Lebanon School District security policies relating to Acceptable Use of IT systems including email, internet, and etc.
- Individual end users are not permitted to open cloud service accounts or enter into cloud service contracts that will initiate a new vendor relationship, manipulate or change existing relationships without the direct approval and input from the district technology coordinator.
- For any cloud services that require individual users to agree to terms of service or usage, the district technology coordinator will review such documents and determine if end users can agree on an individual basis or identify any needed changes. Always check with your IT management to see if any terms of service or usage you are agreeing to have been reviewed.
- Personally owned and managed cloud services will not be supported nor recommended for work-related purposes including the storage, management, manipulation, sharing, or exchange of district related or owned data.