USFR Compliance Report

Information Technology

Buckeye Union High School District

Objective: To determine whether the district adopted an information technology (IT) security framework that aligned with credible industry standards and implemented controls that provide reasonable assurance that its data is accurate and reliable and protected from unintended exposure and consequences. Test work should determine that the district adopted a framework and controls were operating to protect District and student data.

<table>
<tr><td>IT01</td><td>The district maintained an adequate separation of duties in its IT systems that prevented 1 employee from completing a transaction without additional review and approval procedures.</td></tr>
<tr><td>Description</td><td>Scan the District user system access reports and determine the district adequately separated responsibilities among stall for administration, authorization, and operational responsibilities within the separate business systems (i.e., financial accounting system, student attendance system, student payment systems, network, and website) and limited employee access to only those business functions or software necessary to perform their job function. If this was not possible due to the district's limited stall size, determining adequate management review procedures were in place.

If there were incompatible duties or employees with superuser access, indicate in the comments what systems employees had inappropriate access to and what, if any, steps were taken to mitigate the risks of unauthorized changes.</td></tr>
<tr><td>Policy / Procedure</td><td>The district has a workflow that defines the management of accounts and the level of permissions for accounts that facilities for the separation of duties. This is controlled by having one employee that approves accounts to be created/deleted as well as determining the level of permissions. This approval is requested and documented in a log. Then a separate employee physically executes the creation/deletion and assigns permissions. This is done to lower the risk of unauthorized activity.
<table>
<tr><th>System</th><th>Approver (Account/Role)</th><th>Executor</th></tr>
<tr><td>Visions</td><td>Procurement Supervisor (Dawn Hopkins)</td><td>Office of the Maricopa County School Superintendent</td></tr>
<tr><td>Synergy</td><td>Executive Director of IT (Nicholas Magann)</td><td>Student Information Director (Mundi Wallace)</td></tr>
<tr><td>NutriKids</td><td>Director of Budget & Finance (Laurie Colbert)</td><td>Admin Assist III - Business Office (Hilda Alvarado)</td></tr>
</table>
</td></tr>
</table>

	<table><tr><td>TimeClock Plus</td><td>Director of Budget & Finance (Laurie Colbert)</td><td>Payroll/Benefits Supervisor (Mary Wickander)</td></tr><tr><td>InTouch</td><td>Director of Budget & Finance (Laurie Colbert)</td><td>Admin Assist III - Business Office (Vicki Martin)</td></tr></table> System configuration is also tracked using this Application Matrix: Application Matrix.xlsx

IT02	The district reviewed and documented any system or software changes implemented.
Description	Scan the District's procedures and documentation to confirm any modifications to system hardware or software were authorized by a supervisor and were appropriate.
Policy / Procedure	Hardware and software changes are reviewed for the potential impact of changes on the system, ensuring that changes are in compliance with any relevant regulations or standards, and documenting the details of any changes that are made. The purpose of this policy is to help ensure the stability, security, and integrity of the organization's systems and to provide a record of changes that have been made for troubleshooting or auditing purposes. • Overall District Technology - All system and hardware changes in the IT environment are approved by the Executive Director of IT. The changes are logged in a hardware and software change log. • Financial System Specifically – The vendor (Tyler Tech) along with the Office of the Maricopa County School Superintendent completely manages all software and hardware changes associated with the hosting of the district's Finacial System. Link to the Logs: Software and Hardware Changes.xlsx

IT03	The district assessed security risks for its systems and data and provided employees annual security awareness training.
Description	Assessed the risks to District systems and data and implemented procedures to prevent and detect technology-related threats, such as risks to its systems, network, and data through email, internet use, VPN, wireless access, and mobile devices. Provided employees security awareness training at least annually that addressed prevention and detection of technology-related threats (i.e., phone and email phishing, website and ransomware attacks, and data breaches), and detailed instructions regarding how to prevent, identify, and report suspected security risks and incidents.
Policy / Procedure	• Annually employee's complete technology security awareness training via an online platform solution called Vector Solutions along with other required training. This is managed and recorded though the HR department. • A monthly newsletter is sent to all employees which contains the lates updated in security awareness.

	• The district conducts quarterly phishing scenarios, which include follow-up training for those that fail the scenarios. This is done through Microsoft Defenders – Attach Simulation Training. • The district conducts quarterly vulnerability scans on the network. The reports are analyzed and recorded. The summary of each report is recorded with the number of vulnerabilities and the risk score. Then the team meets to discuss action items to mitigate the findings. The mitigation steps are recorded for findings that are fixed. Link to Folder containing the scan reports and mitigations: Vulnerability Scans Link to log of phishing simulation and training: Phishing Scenario Training

IT04	The district immediately and appropriately modified terminated or transferred employees' or vendors' access to all District systems.
Description	Determine if the District has a documented process for modifying or removing user access from all systems (e.g., financial accounting system, student information system, District's network, etc.). Scan the current list of vendors and transferred or terminated employees and determine that access to District systems had been appropriately modified or removed.
Policy / Procedure	Account management of terminated employees happens to secure and manage the digital accounts of employees who have been terminated or separated from the BUHSD. This includes disabling their access to company networks, email, and other systems, as well as changing passwords and revoking permissions. Additionally, steps to retain the data of the terminated employees are taken in case the termination is due to a disgruntled employee who tries to sabotage data. No access to accounts, emails, or files will be allowed after the termination date. If the employee desires to retain any information after termination, they will need to ensure all records are downloaded prior to termination and are used for personal use only after leaving Buckeye Union High School District. • Upon termination, HR sets employees' last day in AD Manager then following that last day the automation disables the account in Active Directory. • A secondary automation then moves disabled accounts to a graveyard and removes all groups and permissions. • Any systems that are tied to login with Active Directory then in turn also have their access removed. Link to full policy: Account Termination Policy for Terminated Employees

Commented [NM1]: @Nicholas Magann add info on vendors

IT05	The district's system software and hardware was physically protected from unauthorized access, theft, and environmental hazards.

Description	Determine the District has physical access controls over sensitive areas such as server rooms or communication closets.
Policy / Procedure	Software is protected through the use of passwords, encryption, and secure login protocols. Hardware is protected through the use of physical locks, surveillance cameras, and secure storage facilities. Additionally, environmental hazards are mitigated through the use of temperature and humidity controls, power backups, and fire suppression systems. • All district IDF and MDFs are keyed to only IT admins that have access to the rooms that contain critical infrastructure. • No access is granted to the IDF or MDF without being assisted by a member of the IT admin team. • All computer software is also locked down to the IT department to install and uninstall software. • Critical Software solutions only have IT admin access. Link to full policy: Physical Security of IT Systems Policy

IT06	The district scheduled and performed data backup-control procedures for all critical systems at least daily, or more frequently, to ensure uninterrupted operations and minimal loss of data.
Description	System backup procedures included: • Test of backup reliability and integrity. • Backup copies were stored in separate facilities or fire-rated containers. • Backups were scheduled for a defined time/period.
Policy / Procedure	The data backup policy is a set of guidelines and procedures that BUHSD follows to ensure that their data is regularly and effectively backed up in order to protect against data loss due to hardware failure, software bugs, human error, or other unforeseen events. This includes specifying how often backups should be taken, what types of data should be backed up, where backups should be stored, and how they should be verified and tested. The policy also includes procedures for restoring data in the event of a disaster or other data loss event. Overview: • Full backups are taken nightly to the UniTrends backup appliance for all critical systems. • Quarterly the district conducts an exercise to restore backups into a sandbox environment to verify the backs and to record the Time to Restore objective. Link to the full back up plan: Backup Plans.docx

Commented [NM2]: @Nicholas Magann create backup policy and link to here

IT07	The district routinely completed software and application updates and patches when they became available.

Description	Determine the District's process and documentation that software (including anti-virus, anti-spyware, and anti-malware software) and applications were updated, and patches were completed timely. In addition, determining systems are up to date to protect the integrity and reliability of the district's data (i.e., web-based applications, accounting, student attendance, and payroll systems).
Policy / Procedure	**Microsoft Updates:** • Featured updates are deferred to 60 days • Quality Patches are deferred to 21 • Critical patches are deferred to 7 days • Microsoft Defender updates every 2 hours. **Tanium** The district leverages Tanium, which is software solution that provides endpoint security and systems management solutions. Tanium is a platform that allows BUHSD to quickly and effectively manage and secure their endpoints, including laptops, servers, and mobile devices. Tanium platform provides the following features : • Real-time endpoint visibility and control • Automated software and patch management • Advanced threat detection and response • Compliance and regulatory reporting • Inventory management and reporting • Software distribution and deployment • Remote control and troubleshooting • Network segmentation and isolation • Automated incident response It also enables BUSHD to quickly resolve endpoint issues and to distribute software updates and patches, making it a powerful tool for managing and securing large enterprise networks. https://www.datashieldprotect.com/tools/tanium **Tanium Patch** gives organizations an efficient and effective way to patch software systems at scale. Once all computer groups have been patched administrators can view the deployment status for patches as well as view historical patch and system data for each machine. • Deploy critical system patches at scale • Immediate patch success/failure display • Customize patch schedules and workflows **Overview**: • All software systems used by the organization will be reviewed for updates on a regular basis.

	• High-priority updates, such as security patches, will be applied as soon as they become available. • Other updates, such as feature enhancements, will be evaluated and installed in a timely manner, but only after careful testing and review. • BUHSD will test updates on a test environment before installing production systems. • Before installing updates, IT staff will verify that the updates are compatible with the organization's existing software and hardware configurations. • IT staff will also ensure that the updates will not cause any disruptions to ongoing business operations. • IT staff will also make sure that backups are made and tested before installing any updates Link to full policy: Software and Application Updates and Patches Policy

IT08	The district had vendor contracts or data-sharing agreements in place with any 3rd parties accessing or hosting District data that addressed controls to support security and processing integrity, and backup procedures if applicable, before data was accessed/shared.
Description	Determine the District's vendor contracts or data-sharing agreements had appropriate security, processing, and backup controls in place. In addition, determine the district appropriately reviewed data accessed or processed by vendors or 3rd parties for propriety.
Policy / Procedure	Link to the folder containing data sharing agreements: Data Sharing Agreements All curriculum applications are vetted using TrustEd Apps (1EdTech) which are vetted for compliance with GDPR, FERPA, COPPA. The dashboard also contains all the Terms of Service/Terms of Use as well as Privacy Policy for all the applications that are used in the district. *Access to this dashboard can be granted if you desire.* • Purpose: The purpose of this policy is to establish guidelines for sharing data within the organization and with external partners. • Scope: This policy applies to all data collected, generated, or maintained by the organization, including personal data and sensitive data. • Data Ownership: The organization owns all data collected, generated, or maintained by the organization. Data may be shared with external partners only with the permission of the data owner and in compliance with all applicable laws and regulations. • Data Access: Access to data will be granted on a need-to-know basis and in accordance with the organization's data access policy.

	• Data Sharing Agreement: External partners must enter into a data sharing agreement with the organization prior to receiving any data. The agreement must specify the terms and conditions of the data sharing, including the purpose of the data sharing, the data to be shared, and the responsibilities of each party. • Data Security: Data must be kept secure at all times and in accordance with the organization's data security policy. All parties must comply with the security measures specified in the data sharing agreement. • Data Retention: Data will be retained for the time period specified in the data sharing agreement or as required by applicable laws and regulations. • Compliance: All data sharing activities must comply with applicable laws and regulations, including data protection and data privacy laws. • Responsibility: The organization will be responsible for ensuring compliance with this policy and will take appropriate action to address any violations. • Regular Review : this policy will be reviewed on regular basis to update as per the changes in laws and regulations.

IT09	The district ensured changes to data in business (i.e., employee information, pay rates) and IT (i.e., user roles,access rights) systems were approved by an authorized individual prior to processing changes.
Description	Determine changes to data were reviewed and approved by a designated employee to ensure the validity, completeness, and accuracy of processed data, and if issues were noted, corrective action was taken.
Policy / Procedure	The district ensures all changes of data in business and IT systems are approved by HR as Visions is the employee's system of record. All changes are approved by HR before that data is allowed to sync or change in any other systems.

IT10	The district enforced data security policies related to passwords and user authentication that aligned with credible industry standards.
Description	Followed a password policy that required strong passwords, screen locks, repeated failed sign-on attempt lockouts, and prohibited sharing of user IDs and passwords along with more modem controls to authenticate user identities. Required multifactor authentication for at least all employees with remote access or administrative access to critical IT systems. See IT FAQ 17. If any critical IT systems are not capable of implementing multifactor authentication, determine the district had compensating controls in place to adequately secure those IT systems and related data.
Policy / Procedure	Link to full policy: Password and User Authentication Policy

IT11	The District's IT systems generated electronic audit trail reports or changed logs with information about electronic transactions that the district reviewed or analyzed regularly to determine transactions' propriety.
Description	If a District IT system does not provide an electronic audit trail function, determine the district documented a process that allowed it to audit transactions.
Policy / Procedure	The district's security team reviews audit logs produced by systems based on the terms in the Audit Logs Review Policy then documented in the Audit Logs Findings. Link to full policy: Audit Logs Review Policy Link to log on findings requiring action items: Audit Logs Findings

IT12	The district monitored and reviewed IT system-generated incident or error reports to identify security threats or other unusual activity and addressed noted issues.
Description	The district had procedures to investigate and respond to activities identified in the audit event/ trail function such as repeat failed logons, or failed access attempts related to information systems; administrative privilege usage, employee credential usage, or third-party credential usage; or suspicious network activity.
Policy / Procedure	The district's security team reviews incidents, errors, warnings, and insights produced by systems based on the terms in the Incident and Error Report Review Policy then documented in the Incident and Error Report Log. Link to full policy: Incident and Error Report Review Policy Link to log on findings requiring action items: Incident and Error Report Log

IT13	The district had recovery and contingency planning documents in place to restore or resume system services in case of disruption or failure that were reviewed and tested at least annually.
Description	The district had planning documents that included the date and method the district used to review the plan (i.e., tabletop discussion, system test, or other method). The plan was tested at least annually to ensure employees understand their responsibilities, identify internal and external vulnerabilities, and take action to update equipment or remedy any issues identified since the last review. (II the District used a third-party vendor for IT support, the district should still have a District-level plan to activate the recovery or contingency plan that is tested at least annually.)
Policy / Procedure	Link to Disaster Recovery / Incident Response : Disaster Recovery.docx