|  |  |  |  |
| --- | --- | --- | --- |
|  | CNE Application Security Standards | Prepared for Cherokee Nation Entertainment | Last updated: 7/23/2024 |

|  |  |
| --- | --- |
| Introduction | This document outlines the minimum functional, architectural and security requirements that applications must meet to be permitted within the corporate environment. These requirements apply to all types of applications, including local applications, web applications, and hosted or Software-as-a-Service (SAAS) applications. This document will also include desired or preferred functionality requirements where appropriate. This application standards document is intended to provide requirements for solutions provided by vendors, partners, and internal resources to ensure consistency and integrity of the applications permitted into Cherokee Nation Entertainment’s environment.  Any requirements not met must be documented and disclosed in writing prior to signing of any agreement between CNE and any other party. Internally the documented exceptions must be included on a Risk Summary Document and signed off by the business owner or primary stake holder.  This document is intended to define standards for application behavior, architecture, security, and compatibility with the CNE corporate environment. The level of detail around the standards themselves are not meant to be an exhaustive detail around each requirement, but readable by industry and technology professionals alike. Any additional details can be provided upon request. The document is also intended to be a living document that will be updated as technologies or other circumstances change. |
| **Contents** | 1. **Identity** 1.1 – Authentication and Authorization   1.2 – User Lifecycle Management  1.3 – Role Based Access Control 1.4 - Credentials Management  2- **Data Protection**  2.1 – Encryption  2.2 – Logging and Monitoring  2.3 - Data Retention  2.4 – Endpoint Protection  3- **Communication**  3.1 - Application Data Transfer/Exchange  3.2 – Client Communication |
| **Identity** |  |
| **Identity 1.1** | **Authentication and Authorization** |
| Cloud/SAAS **Authentication and Authorization** - Required | All Hosted applications must support one of the following identity providers: 1- Forms based login  2- Active Directory / Azure Active Directory / EntraID  3- LDAP (Lightweight Directory Access Protocol) 4- OKTA Single Sign-on (SAML, OAuth, OpenID) 5- Azure Single Sign-on (SAML, OAuth, OpenID)  Hosted applications must support strong authentication mechanisms, such as multi-factor authentication (MFA), for user access, or be compatible with OKTA or Azure as an Identity provider for Single Sign On. |
| Cloud/SAAS **Authentication and Authorization** - Preferred | Our preferred method of user sign-in is Single-Sign-On via OKTA or Azure. This creates the least amount of friction for our users. |
| Local/On-Premises **Authentication and Authorization** - Required | All Local applications (thick client or web based) must support one of the following identity providers:  1- Active Directory / Azure Active Directory / Entra ID  2- LDAP (Lightweight Directory Access Protocol)  3- OKTA Single Sign-on (SAML, OAuth, OpenID)  4- Azure Single Sign-on (SAML, OAuth, OpenID)  5- Windows Authentication  6- Forms Based (must utilize the user’s local Active Directory credentials) |
| Local/On-Premises **Authentication and Authorization** - Preferred | Our preferred method of user sign-in is Single-Sign-On via OKTA or Azure for web-based applications. For thick client applications Windows Authentication is preferred. |

|  |  |
| --- | --- |
| **Identity 1.2** | **User Lifecycle Management** |
| Cloud/SAAS **User Life Cycle Management** - Required | All Hosted applications must support the automated revocation of access to the hosted application. When access for a user account is disabled or deleted in our corporate environment the application must prevent the account from logging in.  The mechanisms for this are typically via the Single Sign-On provider (OKTA or Azure) which is immediate, however if this can be accomplished via a user feed/sync and the information is not sensitive in nature the maximum threshold for revoking access is 24 hours. |
| User Life Cycle Management - Preferred | It is highly preferred that the account within the application is removed or rendered inactive upon the corporate account being disable/deleted. |
| Local/On-Premises User Life Cycle Management - Required | All locally hosted applications must support the automated revocation of access to the hosted application. When access for a user’s account is disabled or deleted in our corporate environment the application must prevent the account from logging in.  The mechanisms for this are typically via the authentication method, which is immediate, however if this can be accomplished via a user feed/sync and the information is not sensitive in nature the maximum threshold for revoking access is 24 hours. |
| Local/On-Premises User Life Cycle Management - Preferred | It is highly preferred that the account within the application is removed or rendered inactive upon the corporate account being disable/deleted. |

|  |  |
| --- | --- |
| **Identity 1.3** | **Role Based Access Control** |
| Cloud/SAAS **Role Based Access Control** - Required | Role-based access control (RBAC) should be implemented to ensure that users have appropriate access privileges based on their roles and responsibilities. The user’s role within the application controls the appropriate level of security for the user. |
| Cloud/SAAS **Role Based Access Control** - Preferred | Role-based access control (RBAC) should be assigned based on an attribute of the user stored in CNE’s corporate user management system. There are several methods to accomplish this, below is a list of supported methods, but this list is not meant to be comprehensive.   1. OKTA or Azure SAML Attribute/Statement ( parsing the SAML assertion of a user, we can pass over any Active Directory attribute or AD group membership with SAML ) 2. Azure AD / Entra ID User attributes (Title, Department, Company, Location etc.) 3. Azure AD / Entra ID Group membership (Custom application groups indicating user role) 4. Active Directory User attributes (Title, Department, Company, Location etc.) 5. Active Directory Group membership (Custom application groups indicating user role) 6. LDAP (Lightweight Directory Access Protocol) 7. Mid-Server Integration, a local server that makes outbound only connections to the hosted platform can pass user information. 8. OKTA OpenID can query user attributes in OKTA (populated via Active Directory) 9. Human Resources Management System. SFTP push from CNE’s system to Cloud/SAAS platform. 10. Human Resources Management System. API integration SaaS to SaaS connection. |
| Local/On-Premises **Role Based Access Control** - Required | Role-based access control (RBAC) should be implemented to ensure that users have appropriate access privileges based on their roles and responsibilities. The user’s role within the application controls the appropriate level of security for the user. |
| Local/On-Premises **Role Based Access Control** - Preferred | Role-based access control (RBAC) should be assigned based on an attribute of the user stored in CNE’s corporate user management system. There are several methods to accomplish this, below is a list of supported methods, but this list is not meant to be comprehensive.   1. OKTA or Azure SAML Attribute/Statement ( parsing the SAML assertion of a user, we can pass over any Active Directory attribute or AD group membership with SAML ) 2. Azure AD / Entra ID User attributes (Title, Department, Company, Location etc.) 3. Azure AD / Entra ID Group membership (Custom application groups indicating user role) 4. Active Directory User attributes (Title, Department, Company, Location etc.) 5. Active Directory Group membership (Custom application groups indicating user role) 6. LDAP (Lightweight Directory Access Protocol) 7. Mid-Server Integration, a local server that makes outbound only connections to the hosted platform can pass user information. 8. OKTA OpenID can query user attributes in OKTA (populated via Active Directory) 9. Human Resources Management System. SFTP push from CNE’s system to Cloud/SAAS platform. 10. Human Resources Management System. API integration SaaS to SaaS connection. |

|  |  |
| --- | --- |
| **Identity 1.4** | **Credentials Management** |
| Cloud/SAAS **Credentials Management** - Required | The application shall never display a user’s password. It shall always be echoed with special characters representing typed characters.   The application must have the ability to log out users after a predetermined amount of inactivity.  The back-end servers shall never display or store a user’s password in clear text. The user’s password will be the same as their corporate password.  No clear text passwords will be stored in cookies, configuration files, system memory or otherwise.  System credentials used for Break-Glass access, API or integration credentials/secrets, or any privileged or administrative function shall only be stored or disclosed to system owners or IT personal responsible for system management and/or configuration. |
| Local/On-Premises **Credentials Management** - Required | The application shall never display a user’s password. It shall always be echoed with special characters representing typed characters.   The application must have the ability to log out users after a predetermined amount of inactivity.  The back-end servers shall never display or store a user’s password in clear text. The user’s password will be the same as their corporate password.  No clear text passwords will be stored in cookies, configuration files, system memory or otherwise.  System credentials used for Break-Glass access, API or integration credentials/secrets, or any privileged or administrative function shall only be stored or disclosed to system owners or IT personal responsible for system management or configuration.  Service accounts will utilize gMSAs (Group Management Service Accounts) where possible. Otherwise “user” service accounts will have a minimum password of 25 characters and must only be allowed to login to hosts required for the system to function properly. |

|  |  |
| --- | --- |
| **Data Protection** |  |
| **Data Protection 2.1** | **Encryption** |
| Cloud/SAAS **Encryption** - Required | All data transmitted between CNE and our Cloud/SAAS applications must be encrypted using industry-standard encryption protocols, such as HTTPS, TLS, and AES.  Additionally, data at rest within the Cloud/SAAS infrastructure is also encrypted using strong encryption algorithms. This means that customer data stored in databases, storage systems, and backups remains encrypted and inaccessible to unauthorized entities. Applications must employ proper data masking techniques to safeguard sensitive information.  Cloud/SAAS solutions must not utilize deprecated cypher suites. |
| Local/On-Premises Encryption - Required | All data transmitted to the application must be encrypted using industry-standard encryption protocols, such as HTTPS, TLS, and AES.  Additionally, sensitive data at rest within the database infrastructure is also encrypted using strong encryption algorithms. This means that sensitive data stored in databases, storage systems, and backups remains encrypted and inaccessible to unauthorized entities. Applications must employ proper data masking techniques to safeguard sensitive information.  Applications must not utilize deprecated cypher suites. |

|  |  |
| --- | --- |
| **Data Protection 2.2** | **Logging and Monitoring** |
| Cloud/SAAS **Logging and Monitoring** - Required | All relevant security events, application activities, and user interactions are logged in a structured and standardized format. Logging should capture information such as timestamp, event type, source IP, user ID, and specific details about the event or action taken.  Logs are retained for a minimum period, as mandated by regulatory requirements or internal specified requirements. Log retention periods may vary based on the type and criticality of the logged data.  The Cloud/SAAS provide must have a process for requesting relevant logs to CNE upon request. |
| Local/On-Premises Logging and Monitoring - Required | All relevant security events, application activities, and user interactions are logged in a structured and standardized format. Logging should capture information such as timestamp, event type, source IP, user ID, and specific details about the event or action taken.  Logs are retained for a minimum period, as mandated by regulatory requirements or internal specified requirements. Log retention periods may vary based on the type and criticality of the logged data.  The logs must be accessible to CNE system administrators. |

|  |  |
| --- | --- |
| **Data Protection 2.3** | **Data Retention** |
| Cloud/SAAS **Data Retention** - Required | Personal, sensitive or compliancy related data collected and stored by the application must be handled in compliance with data protection laws (e.g., HIPAA, GDPR, PCI).  The application’s retention policy must adhere to the strictest requirement of the data stored in the system. |
| Local/On-Premises **Data Retention** - Required | Personal, sensitive or compliancy related data collected and stored by the application must be handled in compliance with data protection laws (e.g., HIPAA, GDPR, PCI).  The application’s retention policy must adhere to the strictest requirement of the data stored in the system. |

|  |  |
| --- | --- |
| **Data Protection 2.4** | **Endpoint Protection** |
| Cloud/SAAS **Endpoint Protection** - Required | N/A |
| Local/On-Premises **Endpoint Protection** - Required | Application endpoints (both client and server) must support the presence of anti-virus/malware real-time protection. |

|  |  |
| --- | --- |
| **Communication** |  |
| **Communication 3.1** | **Application Data Transfer/Exchange** |
| Cloud/SAAS **Application Data Transfer/Exchange** - Required | Data or communications initiated externally must not be allowed from the Cloud/SAAS solution directly to CNE’s datacenter or business networks. Where possible all data exchanged should be initiated from the client or within CNE’s environment creating a stateful connection for data transmission, where this is not possible inbound traffic must connect to a DMZ located server to broker the exchange of data. Services must limit the ports listening to a service to what is used, services should not have open network ports that are not explicitly used for the function of the application.   Business to Business or Cloud to Cloud such as Azure Express Route and other similar technologies or connections must be secure and encrypted No communication in production environment shall be left un-secured and support proper key rotation.  Supported methods and standard of data transmission:  1- SFTP (Secure File Transfer Protocol): SFTP for transmitting files over SSH must use at minimum a “Strong” security level.  2- HTTPS: If data is transmitted over HTTP it must be encrypted over HTTPS and SSL/TLS.  3- SOAP (Simple object access protocol) API (Application Programming Interface): All API communication must be encrypted (HTTPS and SSL/TLS). The API should only expose the minimum amount of data that is necessary to fulfill the requests of its clients.   4- REST (Representational State Transfer) API (Application Programming Interface): All API communication must be encrypted (HTTPS and SSL/TLS). The API should only expose the minimum amount of data that is necessary to fulfill the requests of its clients.  5- VPN (Virtual Private Network) over IPSec(Internet Protocol Secure): This would be uncommon and requires additional infrastructure to facilitate. Point to point IPSec tunnels must uses the strongest encryption supported by each end point and cannot utilize deprecated technology.  6- Azure ExpressRoute – Azure ExpressRoute connections must follow recommended configuration: [Azure ExpressRoute Overview: Connect over a private connection | Microsoft Learn](https://learn.microsoft.com/en-us/azure/expressroute/expressroute-introduction) 7- Azure Networking Services- Azure Private Link and other services must follow recommended configuration: [Azure networking services overview | Microsoft Learn](https://learn.microsoft.com/en-us/azure/networking/fundamentals/networking-overview) |
| Local/On-Premises **Application Data Transfer/Exchange** - Required | On premise systems that leverage external data or communications initiated externally must not be allowed from the Cloud/SAAS solution directly to CNE’s datacenter or business networks. Where possible all data exchanged should be initiated from the client or within CNE’s environment creating a stateful connection for data transmission, where this is not possible inbound traffic must connect to a DMZ located server to broker the exchange of data. Services must limit the ports listening on a service to what is used, services should not have open network ports that are not explicitly used for the function of the application. No communication in production environment shall be left un-secured.  Supported methods and standard of data transmission:  1- SFTP (Secure File Transfer Protocol): SFTP for transmitting files over SSH must use at minimum a “Strong” security level.  2- HTTPS: If data is transmitted over HTTP it must be encrypted over HTTPS and SSL/TLS.  3- SOAP (Simple object access protocol) API (Application Programming Interface): All API communication must be encrypted (HTTPS and SSL/TLS). The API should only expose the minimum amount of data that is necessary to fulfill the requests of its clients.  4- REST (Representational State Transfer) API (Application Programming Interface): All API communication must be encrypted (HTTPS and SSL/TLS). The API should only expose the minimum amount of data that is necessary to fulfill the requests of its clients.  5- VPN (Virtual Private Network) over IPSec (Internet Protocol Secure): This would be uncommon and requires additional infrastructure to facilitate. Point to point IPSec tunnels must uses the strongest encryption supported by each end point and cannot utilize deprecated technology.  6- SQL (Structured Query Language): All SQL communication should utilize TDE (Transparent Data Encryption) and security best practices. |

|  |  |
| --- | --- |
| **Communication** |  |
| **Communication 3.2** | **Client Communication** |
| Cloud/SAAS **Encryption** - Required | Compatibility – Must be compatible with Microsoft Chromium Edge  The customer’s web browser shall never display a customer’s credit card number after retrieving from the database. It shall always be shown with just the last 4 digits of the credit card number. |
| Local/On-Premises **Encryption** - Required | Compatibility – Must be compatible with Microsoft Chromium Edge  The customer’s web browser shall never display a customer’s credit card number after retrieving from the database. It shall always be shown with just the last 4 digits of the credit card number. |