Purpose:

This documentation establishes the criteria for submitting OSN Education Website Whitelist requests within our firewall application to provide incarcerated individuals with limited and secure access to approved web content. It aims to maintain network security, ensure compliance with institutional regulations, and promote constructive digital engagement.

Scope:

This document applies to all personnel, including staff and approved external contractors, responsible for managing internet access within the institution's secure network environment.

URL Criteria for OSN Education Website Whitelist Requests:

All requested URLs for the OSN Education Website Whitelist **must** meet the following criteria to be considered:

1. **Essential for Class Completion:**
   The URL must be absolutely essential for the successful completion of a class or program. The class cannot be taught or completed without access to this specific URL.
2. **Educational or Rehabilitative Purpose:**
   The URL must provide content directly related to educational programs, vocational training, self-improvement, rehabilitation, or legal research.
3. **Security and Safety Compliance:**
   The website must not contain content that could jeopardize institutional security, public safety, or the personal safety of individuals. This includes but is not limited to:
   - No access to personal communication platforms, social media, or unmonitored messaging systems.
   - No content promoting violence, contraband, or criminal activities.
4. **No Dynamic or Interactive Content:**
   URLs with dynamic content such as real-time chats, forums, comment sections, or user-generated content will not be considered unless explicitly reviewed and approved by the Department of Corrections' Cyber Security Unit and Chief Information Security Officer.
5. **Minimal Risk of Malware or Phishing:**
   The requested URL must not pose a cybersecurity threat, including risks of malware, phishing attempts, or suspicious downloads. Requests for URLs from unknown or unverified sources will be denied.
6. **Reviewed and Approved by the local site's Educational Administrator, the Department of Corrections' Cyber Security Unit, and the Educational Director:**
   Requests must be reviewed and approved by the Educational Administrator, the Department of Corrections' Cyber Security Unit, and the Educational Director responsible for overseeing digital resources used for education or rehabilitation.

7. **Institutional Relevance:**
   The content of the URL must align with the institution's goals and policies, providing value to incarcerated individuals in areas such as education, vocational skills, or mental wellness.

8. **No Commercial or E-commerce Access:**
   URLs related to online shopping, financial transactions, or e-commerce platforms will be rejected unless deemed essential for approved vocational training programs.

9. **No Proxy or VPN Access:**
   URLs that allow or encourage bypassing security restrictions, including proxy servers or VPN services, will not be approved.

Submission Process:

1. **Request Form Completion:**
   All requests must be submitted through EasyVista under the correct OSN Education Website Whitelist topic. Only **one** URL may be submitted per EasyVista ticket and wildcard URLs cannot be accepted. Each submitted ticket **must** include the following:

   - The full URL (to include *http://* or *https://*). ***Please note, **NO** wildcard URLs will be accepted as they cannot be scanned by our tools.***
   - A detailed description of the content and purpose of the website.
   - A detailed justification for how the URL meets the criteria outlined in this service request.

2. **Educational Administrator Approval:**
   The educational administrator for each site will conduct an initial assessment of the URL to ensure it meets the outlined criteria for the URL website whitelist request.

3. **Website Approval from Educational Director:**
   Approved initial reviews from Educational Administrators will be forwarded to the Educational Director for further evaluation and approval.

4. **Department of Corrections Cyber Security Unit Review:**
   The Department of Corrections' Cyber Security Unit will conduct a thorough assessment to ensure the URL does not pose security risks or violate institutional policies.

5. **Website URL Entered into Network Firewall:**
   A member of the Department of Corrections Data Networking Services team will enter the approved URL into the website URL whitelist for the network firewall.

6. **Notification:**
   The requestor will be notified of the decision via e-mail through automated EasyVista workflows. Approved URLs will be added to the whitelist and monitored periodically for continued compliance.

Periodic Review and Monitoring:

Whitelisted URLs will be reviewed periodically to ensure they remain compliant with institutional policies and security standards. Non-compliant URLs will be subject to immediate removal.

Violations:

Failure to adhere to this document may result in disciplinary action, including suspension of network access privileges, depending on the severity of the violation.

Effective Date:

This document is effective as of 3-26-25.

Review Cycle:

This document will be reviewed annually or as necessary to maintain security and compliance.

Contact Information:
For questions or clarifications regarding this document, please contact the Department of Corrections Cyber Security Unit.