PIXELVIEW

Pixelview Application Hardening Guidelines

Date: October 1, 2024
Revision: 1.0

Introduction

To ensure the highest level of security when using Pixelview, we recommend applying the following hardening guidelines. These best practices will help protect your content, safeguard user access, and maintain the integrity of your projects.

Hardening Guidelines

1. **Enable Watermarking**
    - Activate watermarking on all video streams to deter unauthorised sharing and easily identify potential leaks.
2. **Use Private Invites Exclusively**
    - Disable Group Links: Prevent access via shared links.
    - Send Private Invites: Only allow access through direct, individual invitations.
3. **Secure Project Management**
    - Set Expiration Dates: Create projects with predefined expiration times so they auto-delete when no longer needed.
    - Delete Completed Projects: Remove projects after completion to minimise data exposure.
    - Pause Inactive Streams: If taking a break, pause the stream to prevent it from remaining open unnecessarily.
4. **Implement Multi-Factor Authentication (MFA)**
    - Use SMS Verification or through Google/Apple/SSO: Enhance account security by enabling MFA when signing in.
5. **Monitor Active Viewers**
    - Regularly check the list of active viewers during streams.
    - Immediately remove any unknown or unauthorised users.
6. **Manage Access Control**
    - Limit Administrative Access: Minimise the number of users with access to your encoders.
    - Disable Unused Accounts: Remove unnecessary, unused, or unsecure user identities promptly.

- Regularly Review Permissions: Audit user access rights periodically and adjust as necessary.

7. **Ensure Secure Authentication**
   - Use Strong Passwords: Encourage the use of complex passwords that are changed regularly.
8. **Session Management**
   - Log Out After Use: Always log out of the admin portal and other sessions when finished.
9. **Maintain System Security**
   - Install Antivirus/Anti-Malware: Ensure all devices accessing Pixelview have up-to-date security software according to internal recommendations.
   - Keep Systems Updated: Regularly update operating systems and applications with the latest security patches.
10. **Follow Testing Procedures**
    - Pre-Deployment Testing: Test all functionalities on non-production content before deploying Pixelview into production.
11. **Regularly Review Guidelines**
    - Annual Updates: Review and update these hardening guidelines annually or when system components are installed or upgraded.

Conclusion

By following these guidelines, you enhance the security of your content and ensure a safe and efficient experience with Pixelview. We are committed to providing you with a secure platform and appreciate your partnership in maintaining these standards.

Max Stromberg
Chief Executive Officer
Pixelview

Note: This document is intended to provide best practices for securely using Pixelview. For any questions or additional support, please contact our customer service team at hello@pixelview.io.