Login &
Sharing Security

ioGates
CLOUD BASED VIDEO MANAGEMENT

1

USERNAME:
user@example.com
PASSWORD:
XXXXXXXXXX____

2

YOUR PIN IS
5555

3

ENTER YOUR PIN
5555 CONFIRMED ✓

- Two Factor Authentication for ioGates backend users and for share links, this means that Two Factor Authentication protects all access to your ioGates account
- Optional Digital Rights Management (DRM) protected video streaming using Intertrust ExpressPlay
- Using Personalized Watermarking the preview proxy video will have the share receiver's email address burned in
- ioGates supports Single Sign On for Enterprise plans

ja@iogates.com

00:00:02:02   DRM

IT Assets

- We perform third party security assessment
- Sub-dependencies are checked for security and performance issues
- We follow strict compliance with source code licensing and open-source licensing

Management of Access Keys

- **ioGates.com** maintains a strict policy for assigning and distributing keys which may access any production or development systems
- Access keys are never stored in any version control system
- Access keys are never stored anywhere as plaintext
- Individual access keys are generated per employee with developer only access

Remote Access Control and Encryption

- End-to-end 256 bit HTTPS SSL Encryption using Extended Validation (EV) Certificates
- All non-essential ports and links to external network interfaces are blocked by default
- Plan against security threats, vulnerabilities, and risks
- Account passwords are stored with hashes
- Client communication sessions, are validated server-side
- ioGates do not store financial data or credit card information

- All power and networking have redundant failovers to prevent service disruptions
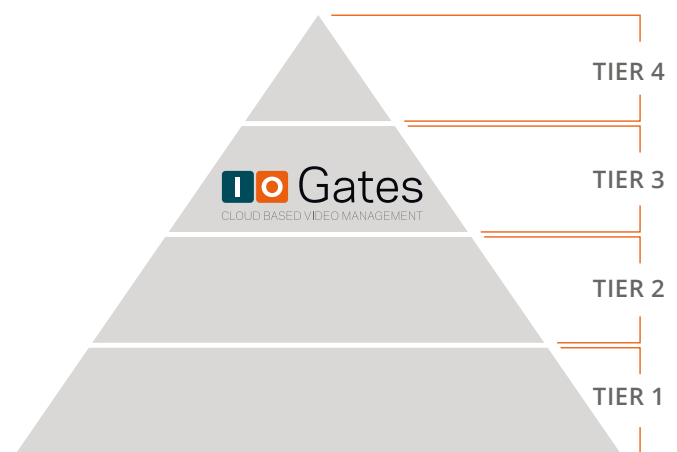
Laptops and mobile devices

- All company laptops use encryption for storing of any potentially sensitive data
- All company laptops use anti-malware and antivirus software

Employees

- ioGates employees are instructed in best practice security standards
- ioGates developers only work with anonymized data

Data center

- ioGates hardware is co-located in Interxion Copenhagen data center
- Interxion Copenhagen is ISO 27001 and SOC2 compliance
- ioGates server location at within the Interxion data center is Tier 3 certified

Data Center Tiers