Hong Kong Protection of Critical Infrastructures (Computer Systems) Ordinance Requirements Checklist

Discover how FileCloud can support the Protection of Critical Infrastructures (Computer Systems) Ordinance, based on proactive compliance requirements mapping by Cloud Systems Asia.

FileCloud is an enterprise-grade file sharing and content governance solution that offers controlled data sharing and collaboration tools for government departments and agencies around the world. Cloud Systems Asia is a trusted FileCloud partner specializing in data storage, protection and management solutions for organizations in the Asia-Pacific region.

Read our checklist to learn how FileCloud and Cloud Systems Asia can protect critical infrastructures and computer systems, while facilitating secure data storage and exchange.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(1) Reporting of material changes to critical computer systems	FileCloud maintains and communicates official release notes that outline updates to the platform, architecture, or features. Additionally, FileCloud maintains a software lifecycle policy to help customers understand the phases of the FileCloud product lifecycle to assist in technical operations planning for their environments.
(2) Independent computer system security audit	FileCloud provides compliance officers, IT admins, and CTOs with comprehensive audit logs that can be exported as a form of documentation for external regulatory audits. These logs track user identity, action, means of access, geolocation, and time of action for secure monitoring and maintenance of critical computer systems. FileCloud has gone through both SOC 2 type 1 and ISO 27001:2022 certification audits conducted by third parties - documentation on FileCloud's security posture are available upon request from the FileCloud Trust Center.
(3) Security risk assessment	FileCloud goes through extensive penetration testing conducted by a third party prior to major releases and have established and implemented a vulnerability management process to ensure any identified security gaps or vulnerabilities are assessed, categorized, and addressed in a timely manner and according to the severity of vulnerabilities.
(4) Computer System Security Management Plan	
1. Organization, authority, roles, and responsibilities of the computer system security management unit;	FileCloud provides granular access control to set up rules determining who can see what data and what actions they can take. The following methods can be configured to ensure effective access control in FileCloud.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(4) Computer System Security Management Plan *(continued)*	
1. Organization, authority, roles, and responsibilities of the computer system security management unit;	**Granular permissions to folders:** FileCloud can be set up with permissions to team folders to specify who has access to each folder and whether they have the ability to view, edit, share, delete, and manage each folder. FileCloud admins can also give users the ability to set up granular permissions to the folders in their My Files folder. **Role-based access control (RBAC):** In role-based access control (RBAC), admin user roles are given access to different actions and information in the system. **Set expiration dates for temporary users:** Admins and users can share data with expiring access permissions. This is useful for organizations that collaborate with temporary workers, such as contractors. Admins can also disable the user account and enable it again later.
2. Appropriate professional qualifications of the supervisor of the computer system security management unit;	N/A This is not within the scope of the FileCloud platform; however, the FileCloud website offers support and technical documentation that managers and supervisors can review to further their system knowledge.
3. Factors that an Operator of Critical Infrastructure ("CIO") should consider in formulating the policies, standards and guidelines, such as its own requirements on security, the CoP and relevant requirements set out by statutory bodies for individual sectors;	FileCloud's Data Leak Prevention (DLP) and Smart Classification work together to enhance data security and compliance. DLP controls user access and sharing of sensitive files, helping protect PII, PHI, and PCI data to comply with data privacy requirements (e.g., HIPAA and GDPR). Smart Classification automatically scans and tags files based on content, enabling seamless integration with DLP for targeted protection and streamlined security workflows.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(4) Computer System Security Management Plan *(continued)*	
4. How risks related to the operator, and its critical computer system ("CCS") can be identified, assessed, mitigated and monitored while formulating a computer system security risk management framework;	
5. Establish a monitoring and detection mechanism **a. to define a baseline of normal behavior in the operation of the CCS and monitor anomalies against this baseline;** **b. to put in place procedures and processes to respond continuously and in a timely manner to any computer system security incidents received by the monitoring system;** **c. to establish mechanisms and processes to continuously collect and analyze information or intelligence relating to information security threats, including attacker methodologies, tools and technologies involved, and appropriate mitigation actions that can be taken;** **d. to conduct regular review of the monitoring mechanism (at least once every two years) to ensure that it is still effective with response to its nature and technology advancement;**	FileCloud's audit logs give administrators quick visibility into site activity, such as new account creation, user logins, search trends, and file uploads/downloads. For deeper analysis and threat detection, FileCloud can forward these events to third-party Security Information and Event Management (SIEM) systems. This integration can help centralize alerts and audit data, helping organizations monitor and respond to potential security issues more effectively.
6. Computer system security training: taking into consideration the roles of all personnel involved in the operation of the CI, including vendors, contractors and service providers to formulate training programs on various computer system security approaches;	This is not within the scope of FileCloud's platform; however, the FileCloud website offers support and technical documentation. Additionally, FileCloud conducts internal security awareness trainings for all team members as part of onboarding and annual refresher trainings.
7. Adopt a "Security by Design" approach to ensure that security is an integral part of the CCS across its entire lifecycle;	FileCloud adopts a "Security by Design" approach by implementing a secure Software Development Lifecycle (SDLC) policy that guides our development and maintenance processes. This policy outlines a structured framework that includes regular reviews and updates to ensure our software remains secure and aligned with industry best practices.
8. Implement asset management to ensure that an up-to-date inventory of CCS and other associated assets are properly owned, kept and maintained, and restricted for access on a need-to-know basis;	FileCloud's Remote Client Management (RCM) empowers administrators to manage connected client devices with precision. Admins can block specific devices from accessing the server or remotely wipe FileCloud folders to protect sensitive data.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(4) Computer System Security Management Plan *(continued)*	
9. Implement access control and account management: only authorized users and computer resources access control system are allowed to access the CCS while enforcing the least privilege principle; conduct review periodically; revoke all user privileges and data access rights that are no longer required; and maintain logs of all accesses and attempted accesses to the CCS;	FileCloud offers multiple authentication options to ensure only authorized users can access data. Administrators can enable two-factor authentication (2FA) for both browser and mobile logins, applicable to Full and Guest accounts. Supported authentication modes include: • Default Authentication • Active Directory • LDAP • Single Sign-On (SSO)
10. Implement privileged access management to ensure that personnel only have access to the specific administrative capabilities needed; regular reviews on usages of privileged accounts should be conducted by an independent party;	FileCloud gives administrators powerful tools to control who can access data and what actions they can take. Granular folder permissions allow admins to define view, edit, share, and delete rights for Team Folders and personal files. Role-Based Access Control (RBAC) assigns system privileges based on user roles, while policies apply specific permissions to designated users or groups. Additional access controls include: • Expiration dates for temporary user accounts • DLP rules to restrict downloads based on user criteria • Share settings to enforce proper permissions
11. Implement cryptographic key management to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of the information;	FileCloud ensures that information is fully encrypted with TLS 1.4 protocols and AES-256 encryption when it is transmitted and stored, respectively. Only the correct user with the appropriate permissions and decryption key can decrypt the data. To protect login credentials, user passwords are hashed using the secure SHA-1 hash algorithm.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(4) Computer System Security Management Plan *(continued)*	
12. Implement password management by defining a strong password policy;	FileCloud allows administrators to enforce granular password settings tailored to organizational security requirements. Available configurations include: • Minimum password length • Strong password enforcement • Block commonly used passwords • Account lockout after failed attempts • Lockout duration settings • Password expiration timelines • Mandatory password change for new accounts • Password reuse restrictions • Reset attempt intervals • Automated reset password emails
13. Implement physical security to ensure that data centers and computer rooms are located in a comprehensively protected environment;	FileCloud's offers on-premises and cloud deployments, as well as hybrid cloud solutions that provide the best of both worlds: the security of an on-premises EFSS solution with the ease of use and efficiency of cloud technology.
14. Implement system hardening by adopting both the least functionality principle and least privilege principle; the baseline configuration of computer systems should be developed, maintained and reviewed regularly;	FileCloud adopts a system hardening approach based on the principles of least functionality and least privilege. We have documented a comprehensive security checklist available from our support documentation including recommendations to disable unnecessary services, restrict access, and enforce role-based permissions. Baseline configurations are developed using recommended security settings and are regularly reviewed to ensure they remain effective. This includes strong authentication, encryption, and secure sharing controls—all designed to minimize risk and maintain a secure operating environment.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(4) Computer System Security Management Plan *(continued)*	
15. Implement change management: the CIO should plan, monitor and follow up changes to production systems properly, and should back up system files and configurations adequately;	FileCloud allows admins to configure automatic backup settings for users' files and folders to ensure data is secure. Additionally, by default, automatic database backups are enabled. An administrator can change the location where backups are stored, the number of backups to maintain, and the number of days between backups. If a back-up strategy is already implemented, admins can disable automatic backups in FileCloud.
16. Implement patch management by adopting a risk-based approach to promptly devise the appropriate patch management strategy for the CCS;	FileCloud adopts a risk-based approach to patch management by leveraging FileCloud's structured release and update process. Each release includes detailed notes outlining enhancements, fixes, and known vulnerabilities, along with security advisories to guide administrators in applying patches promptly and effectively.
17. Develop appropriate policies and procedures for remote connection;	FileCloud's Smart DLP allows the user to exert control over how much access is granted to which parties. Administrators can choose whether other users are allowed to download, share, or login based on different criteria such as IP range, IP address, user type and group, email domain, folder path, metadata of the document, and user access agents like OS and browsers.
18. Develop management policies for portable computing devices and removable storage media;	FileCloud provides centralized device management and policy-based controls for user access, storage quotas, and file handling, which can indirectly support secure use of portable computing devices. Administrators can selectively block a specific client device from logging into the FileCloud server using FileCloud's RMC function.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(4) Computer System Security Management Plan *(continued)*	
19. Implement backup and recovery policies to ensure the resilience of the system;	FileCloud supports automatic backups for user data and databases by default, with configurable options for storage location, retention, and frequency. Administrators can tailor these settings to align with existing backup strategies or disable them if an external solution is in place.
20. Implement network security control to allow only authorized traffic to enter the network;	FileCloud supports IP-based access restrictions, allowing administrators to limit access to both the admin and user portals by specifying allowed or denied IP addresses. Additional controls include enforcing TLS 1.2/1.3 with strong ciphers, disabling insecure HTTP methods, and managing port configurations to reduce exposure. These measures help maintain a secure perimeter and ensure that only trusted sources can interact with the system.
21. Adopt application security measure such as version control mechanism and separate of environments for development, so as to maintain integrity of an application;	FileCloud supports unlimited file versioning, allowing users to upload changes and maintain historical versions of files. This ensures data integrity by enabling rollback to previous versions and preventing accidental overwrites. Admins can configure how many versions to retain per file, optimizing storage and control. Additionally, FileCloud supports multi-tenancy and multiple instance deployments, which allow organizations to simulate isolated environments for development, testing, and production.
22. Implement log management: the CIO should provide sufficient information to support the comprehensive audits of the effectiveness and compliance of security measures;	FileCloud provides robust log management capabilities to support comprehensive audits of security effectiveness and compliance. Every system action—such as logins, file access, sharing, and configuration changes—is automatically recorded with detailed metadata, including user identity, timestamp, IP address, and access method.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(4) Computer System Security Management Plan *(continued)*	
22. Implement log management: the CIO should provide sufficient information to support the comprehensive audits of the effectiveness and compliance of security measures;	Administrators can search, filter, and export logs for analysis or reporting. FileCloud also integrates with third-party SIEM solutions, enabling centralized monitoring and advanced threat detection. These features ensure that organizations have the visibility and data needed to meet audit requirements and maintain a secure environment.
23. Implement cloud computing security to ensure proper protection; the shared responsibility for information security between the cloud service provider and the organization should be clearly defined and implemented;	FileCloud enforces a robust cloud security framework grounded in system hardening principles, including least functionality and least privilege. A comprehensive security checklist guides the disabling of non-essential services, access restrictions, and enforcement of role-based permissions. Baseline configurations are built on recommended security settings and are regularly reviewed. Security controls include strong authentication, encryption, and secure sharing policies.
24. Implement supply chain management by defining and establishing processes and procedures, through which the confidentiality and non-disclosure agreements are properly managed and reviewed.	The platform does not include supply chain management. However, FileCloud's ISO 27001:2022 certification requires for us to establish a vendor security risks policies and processes.
(5) Incident Response Obligations	
1. Computer system security drills	FileCloud support documentation recommends a list of security settings that can be reviewed at scheduled times to ensure the FileCloud system's security is continuously maintained and to help plan incident response drills. This resource is available through Regular Security Checks - FileCloud Docs - Online.

Protection of Critical Infrastructures (Computer Systems) Ordinance – Proactive Compliance Mapping with FileCloud and Cloud Systems Asia (CSA)

CSA Recommendations	FileCloud Support
(5) Incident Response Obligations *(continued)*	
1. Computer system security drills	Internally, FileCloud maintains a comprehensive Security Incident Response Program, supported by a documented plan that outlines procedures for identifying, managing, and responding to security incidents. A dedicated Security and Disaster Response Team (SDRT) oversees incident handling to ensure timely, coordinated actions that minimize impact and mitigate risk. The plan includes processes for detection, reporting, verification, assessment, containment, and post-incident recovery. To ensure its continued effectiveness, FileCloud conducts an annual incident response test and regularly review and update the plan in line with evolving threats and best practices.
2. Appointment of 24/7 contact point	FileCloud offers various levels of support and service entitlements for Customers worldwide. FileCloud Support can be reached via Ticket Submission Form through login to the Customer Support Portal.
3. Scope of the emergency response plan	FileCloud's audit logs give administrators quick visibility into site activity, such as new account creation, user logins, search trends, and file uploads/downloads. For deeper analysis and threat detection, FileCloud can forward these events to third-party Security Information and Event Management (SIEM) systems. This integration can help centralize alerts and audit data, helping organizations monitor and respond to potential security issues more effectively.
4. Requirements for reporting computer system security incidents	

125 Park Avenue FL 25
New York, NY 10017-5550

Phone: U.S: +1 (888) 571-6480
Fax: +1 (866) 824-9584

https://www.filecloud.com

Copyright Notice

About FileCloud

A privately held software company, headquartered in New York, New York, USA, FileCloud is helping organizations thrive by providing hyper-secure content collaboration and processes solutions. FileCloud is used by millions of customers around the world, ranging from Global 1000 enterprises, educational institutions, government and defense, manufacturing, managed service providers and more.

1M+
USERS

3000+
ENTERPRISES

100+
PARTNERS

90+
COUNTRIES

About Cloud Systems Asia (CSA)

Cloud Systems Asia Limited is a value-added distributor of innovative IT solutions, specializing in data storage, data protection and data management solutions. Through extensive technology and marketplace knowledge, CSA executes the due diligence necessary to select renowned brands and leading edge technologies that provide customers with an opportunity to differentiate in a crowded market.