Digital Policy Office

DATA CENTRE SECURITY

Practice Guide

on

Data Centre Security

Version 1.0
[Public Version]

November 2024

COPYRIGHT NOTICE

Amendment History

Change Number	Revision Description	Pages Affected	Revision Number	Date
-	Release version	-	1.0	November 2024

Proprietary Notice

This Practice Guide on Data Centre Security (“Practice Guide”) is based on the Government internal practices and experiences gained by the Digital Policy Office (“DPO”) and may not be applicable to all situations in the data centre industry. While DPO endeavours to keep the information up to date and correct, DPO makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to this Practice Guide or the information, products, services, or related graphics contained in this Practice Guide for any purpose. In no event shall DPO be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising out of, or in connection with, the use of this Practice Guide by any party.

TABLE OF CONTENTS

1. Introduction

A data centre is the place where IT equipment of one or more enterprises are hosted to run IT systems to collect, transmit, process, store and output data of business processes or e-services of the client enterprises. Apart from the IT servers, networks and storage, a data centre is also accommodated with infrastructures and facilities for power distribution and environmental control as well as the necessary levels of resilience and security required to protect the IT systems service availability. As data is a key element of new production in the digital era that ushers in innovation and drives high-quality development of the digital economy, the integrity of data and services delivery can be mission critical to enterprises and have to be adequately protected.

To leverage the strategic role played by data in driving transformation and high-quality economic development, the Innovation, Technology and Industry Bureau ("ITIB") published the **Policy Statement on Facilitating Data Flow and Safeguarding Data Security in Hong Kong ("Policy Statement")** in December 2023. Data centres play a significant role to provide secure facilities for hosting IT systems and data. With more and more business processes and services delivery being migrated online, data centre security is therefore crucial in protecting data assets and enabling high service availability of IT systems for supporting day-to-day business operations and delivery of digital services. A comprehensive and consistent set of practices for securing a data centre from the design stage to the ongoing operation stage should help mitigate security risks in the data centre and optimise service availability and reliability.

This Practice Guide highlights the objectives and best practices of data centre security, covering different aspects ranging from security management practices to the design and operational practices under a **defence-in-depth** security protection strategy to prevent, detect, respond to and recover from security incidents.

This Practice Guide is a living document, which will be reviewed periodically to reflect new developments of industry best practices for data centre security management and changes in the security landscape of Hong Kong as well as the Government policies and guidelines.

1.1. Objective of the Practice Guide and Intended Audience

This Practice Guide is intended for IT professionals and data centre operation practitioners to support the senior management of data centres in the formulation of their organisational security policies on their data centre(s) and the implementation of sufficient security protection measures in the design and construction of data centre(s) (no matter whether they are *en bloc* buildings or floor level data centres), or in the process of selecting and procuring data centre services from the market, and in the ongoing operations of their data centres.

1.2. Using the Practice Guide

Data centre service providers can make references to the practices proposed in this Practice Guide, and adopt the necessary practices in their data centres as appropriate. The practices mentioned in this Practice Guide have consolidated the experience in the Government as well as best practices of the data centre industry. Data centre service providers should consider the relevancy and associated implications of the practices to their own environment and decide whether the practices mentioned in this Practice Guide are to be adopted or not.

The practices proposed in this Practice Guide are, however, not intended to be definitive nor exhaustive as data centre security management in respective data centres may differ depending on individual business environments. Data centre service providers may make necessary adaptations to meet their specific business needs.

1.3. Conventions

The following is a list of conventions used in this Practice Guide.

Shall	The use of the word ‘shall’ indicates an essential practice or requirement.
Should	The use of the word ‘should’ indicates a practice which should be implemented whenever possible or as far as possible.
May	The use of the word ‘may’ indicates a desirable practice.

1.4. Normative References

The following referenced documents are indispensable for the application of this document.

a) Baseline IT Security Policy [S17], DPO, HKSARG (2024)

b) IT Security Guidelines [G3], DPO, HKSARG (2024)

c) ISO 31000:2018 Risk Management – Guidelines, International Organization for Standardization (2018)

d) GB/T 24353-2022 Risk Management - Guidelines (風險管理指南), Standardization Administration of China (2022)

e) Practice Guide for Security Risk Assessment and Audit [ISPG-SM01], DPO, HKSARG (2024)

f) Practice Guide for IT Security Risk Management, DPO, HKSARG (2024)

g) ISO/IEC 27001-1:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements, the International Organization for Standardization and the International Electrotechnical Commission (2022)

h) ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls, the International Organization for Standardization and the International Electrotechnical Commission (2022)

i) ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks, the International Organization for Standardization and the International Electrotechnical Commission (2022)

j) ISO/IEC 22237-1:2021 Information Technology — Data centre facilities and infrastructures — Part 1: General concepts, the International Organization for Standardization and the International Electrotechnical Commission (2021)

k) ISO/IEC 22237-2:2024 Information Technology — Data centre facilities and infrastructures — Part 2: Building construction, International Organization for Standardization and the International Electrotechnical Commission (2024)

l) ISO/IEC 22237-3:2021 Information technology — Data centre facilities and infrastructures — Part 3: Power distribution, the International Organization for Standardization and the International Electrotechnical Commission (2021)

m) ISO/IEC 22237-4:2018 Information technology — Data centre facilities and infrastructures — Part 4: Environmental control, the International Organization for Standardization and the International Electrotechnical Commission (2018)

n) ISO/IEC TS 22237-5:2018 Information technology — Data centre facilities and infrastructures — Part 5: Telecommunications cabling infrastructure, the International Organization for Standardization and the International Electrotechnical Commission (2018)

o) ISO/IEC 22237-6:2024 Information Technology - Data centre facilities and infrastructures — Part 6: Security systems, the

International Organization for Standardization and the International Electrotechnical Commission (2024)

p) GB50174-2017 Code for design of data centers (數據中心設計規範), the Ministry of Housing and Urban-Rural Development of the People's Republic of China (2017)

q) ANSI/TIA-942-C Telecommunications Infrastructure Standard for Data Centers, Telecommunications Industry Association (2024)

2. Data Centre Security Objectives

2.1. Data Centre Security Objectives

Data centre security must meet the objectives of protecting the data assets and service availability of all the IT systems hosted in the data centre, in particular the ones with the highest criticality and data sensitivity. This Practice Guide aims to provide guidelines for facilitating data centre service providers in building or selecting the data centre and to formulate ongoing operations that meet their security requirements, mainly focusing on risks and threats to the data centre that have impacts on the two key areas: Data Security and Service Availability. In contrast with information system security which protects data assets and IT services on the computer, storage, network and software level, data centre security in the context of this Practice Guide focuses mainly on **physical security** of the data centre premises, though there are information system security concerns in common with traditional information systems when many data centre management and control systems are IP network connected and running on general-purpose operating systems like Windows and Linux.

2.1.1. Objectives in the Data Security Key Area

Data centre security should protect data assets held by the IT systems hosted in the data centre against unauthorised access, disclosure, alteration, destruction or loss.

Data security attack surfaces can be broadly categorised into cyber and physical types. This Practice Guide primarily focuses on the protection of physical attack surfaces, providing physical security for the data centre premises. Data centre service providers should follow relevant information security standards or best practices (such as ISO/IEC 27001 or by making reference to the Baseline IT Security Policy [S17], DPO, HKSARG (2024) and the IT Security Guidelines

[G3], DPO, HKSARG (2024)) to safeguard data security of their data centres against threats from cyberattack surfaces.

2.1.2. Objectives in the Service Availability Key Area

Data centre security should protect the availability of the data centre hosting services and facilities against attacks that may impact the IT services to be delivered by the IT systems hosted in the data centre. The service availability key reference points for data centre include the availabilities of power, cooling, fire-fighting, server, network and storage facilities.

3. Core Security Management Principles

This section introduces some generally accepted principles that address data centre security from a high-level viewpoint. These principles are fundamental in nature and rarely change. Data centre service providers shall observe these principles for designing, building and operating their data centres. The principles listed below are by no means exhaustive.

3.1. Risk Based Approach

A risk based approach shall be adopted to identify, prioritise and address the security risks of data centres in a consistent and effective manner. Proper security measures should be implemented through a risk management system, e.g. ISO 31000 or GB/T 24353, adopted by data centre service providers to protect their assets and mitigate security risks to an acceptable level.

3.2. Security by Design Approach

A security by design approach shall be adopted to incorporate security requirements into the design processes of a data centre, ensuring that data centres are implemented with appropriate security measures and resilience. Security shall be considered and introduced throughout all phases of the design processes in order to minimise rework efforts.

3.3. Prevent, Detect, Respond and Recover

Data centre security is a combination of preventive, detective, response and recovery measures. Preventive measures avoid or deter the occurrence of an undesirable event. Detective measures identify the occurrence of an undesirable event. Response measures refer to co-ordinated actions to contain damages when an undesirable event / incident occurs. Recovery measures restore the confidentiality, integrity and availability of information systems to their expected state. Data centre service providers shall designate appropriate personnel to manage data centre security as well as data centre security incident handling.

3.4. Continual Improvement

To be responsive and adaptive to changing environments and technologies, a continual improvement process shall be implemented for monitoring, reviewing and improving the effectiveness and efficiency of data centre security management. The performance of security measures shall be evaluated periodically, e.g. via physical penetration test and intrusion exercise, etc., to determine whether the data centre security objectives are met. Meanwhile, data centre service providers should stay up-to-date on the latest security incidents, both domestic and overseas, as these incidents may directly impact the security, reliability and operation of data centres. Data centre service providers can also use these incidents as references to review any similar security loopholes that may exist in their own data centres and take steps to prevent them from happening.

4. Data Centre Security Management Considerations

4.1. Data Centre Security Management Organisation Structure

Like the security management of information systems, the effective implementation of a security strategy must have an effective security management organisation structure to oversee and steer the implementation and ongoing operations of various security protection measures to protect critical assets of the data centre.

Data centre service providers shall establish a dedicated security management organisation structure with sufficient authority and competencies to oversee and manage the security of their data centres from both physical and cyber sides. The security management organisation structure shall develop and implement their own security policies and procedures to safeguard the security of their data centres. A security incident response team and response mechanism shall be established for coordinating, communicating, handling and escalating security incidents.

Data centre service providers may make reference to the Baseline IT Security Policy [S17], HKSARG (2024) for setting up their organisation structure for data centre security management.

4.2. Risk Assessment and Management

The ultimate goal of security protection for a data centre is to protect the assets of the data centre. To devise the security requirements of a data centre, data centre service providers should first identify its assets (at an appropriate level of detail) and their values so as to set the target of security protection for them. Each asset shall be assigned to an owner.

The security protection requirements of a data centre should be determined by the data centre service providers responsible for data centre assets, following a risk assessment based on the assets to be protected (according to their **asset value**), weighed with their potential risk (i.e. the **likelihood** through **threat analysis** and **vulnerability analysis**).

The baseline risk posed to the data centre should be identified during the risk assessment process. Appropriate technical, physical and procedural countermeasures or a combination of these countermeasures should be employed to manage the identified baseline risk.

After the deployment of baseline countermeasures, the following risk treatment decisions shall be taken against the residual risk(s) in accordance with the risk tolerance range of the asset owner: (a) acceptance; (b) reduction; (c) transferral; and (d) avoidance.

Regular threats and vulnerability risk assessment should be conducted to identify any potential security threats and operational weaknesses in the data centre.

5. Data Centre Security Design Considerations

The application of physical security measures to the facilities and infrastructures of a data centre has a direct impact on both the availability of the data centre and the integrity/security of the data assets stored and processed within it.

5.1. Service Availability Considerations

The service availability of a data centre depends on the service availability of its facilities and infrastructures. The service availability design for data centre facilities and infrastructures could be generally classified into four classes:

Class	Technical solution
1	Single path
2	Single path with redundancy
3	Multiple paths providing concurrent maintainability
4	Multiple paths providing fault-tolerant

The service availability class shall be selected for the following infrastructures, based on the outcome of the business risk assessment, during the design phase of a data centre: (a) power supply and distribution; (b) environmental control (e.g. cooling system); and (c) telecommunications cabling.

More information can be found in the references mentioned in Section 1.4 such as ISO/IEC 22237 series.

5.2. Physical Security Considerations

The physical security of the data centre will influence both the probability and impact of risk events, since the objective of physical security is to protect against:

a) Unauthorised access;
b) Intrusion;
c) Internal environmental events (e.g. overheating, fire, water leakage, etc.);
d) External environmental events (e.g. fire, flood, explosion and other forms of natural disaster, etc.); and
e) Insider threat.

Access control and intrusion prevention measures of a data centre should be implemented according to the purpose of the data centre and the functionality of the data centre areas and pathways.

Protection against internal and external environmental events includes all measures required to maintain the desired service availability class for the data centre facilities and infrastructures, including building construction, security installations and organisation measures.

More information can be found in the references mentioned in Section 1.4 such as ISO/IEC 22237 series.

5.3. Multi-zoned Concept

Multi-zoned concept and considerations should be adopted to facilitate access control design of data centres:

a) Areas within the data centre should be divided logically into different security zones and areas according to operational needs;
b) Zones and areas should be subject to different security measures and access control depending on the values and vulnerabilities of assets within;
c) Access rights shall be defined according to the roles and responsibilities of personnel; and
d) Pathways to the data centre infrastructures (e.g. data hall, plant areas and telecommunications cabling) shall be designed to prevent unauthorised passage between different security zones

and areas, in particular from a lower security zone/area to a higher security zone/area.

5.4. Business Risk Analysis

The design of each of the data centre facilities and infrastructures shall take account of their impact on overall service availability and the costs associated with the predicted downtime associated with failure or planned downtime for maintenance.

The design and physical security of the facilities and infrastructures of a data centre shall be subjected to a risk analysis which maps identified risk events against the requirements of the service availability classification of the facilities and infrastructures.

A business risk analysis identifies the aspects of the facilities and infrastructures that require investment in terms of design improvements to reduce their impact and/or probability of those risk events.

5.5. Site Level Security Design Considerations

Site level security design considerations listed in the following which are mainly related to environmental factors should be taken into account.

a) The environmental factors mentioned in Annex C – Data Center Site Selection and Building Design Considerations of the ANSI/TIA-942-C Telecommunications Infrastructure Standard for Data Centers, Telecommunications Industry Association ("TIA") 942-C Standard; and some relevant risk factors are listed below for consideration:

Source of risks	Impact
Proximity to flood hazard area	Flooding of data centre

Source of risks	Impact
Proximity to major highway traffic arteries	Truck crash led to explosion
Proximity to electromagnetic interference such as electrical power supply station and radar transmitter	Electromagnetic energy that has an undesirable effect on sensitive electronic equipment or signal transmissions
Next to high risk facilities such as oil pipelines, refineries, chemical factories, gas stations, compressed gases distributors and the like	Explosion from gas or other chemical

b) Site for critical data centre should have the resilience of power supply and distribution, telecommunications paths from multiple telecommunications operators, cooling supply paths (if district cooling system is used), etc. so that services delivery can be maintained when the primary path is blocked for whatever reasons; and

c) For data centres hosting mission critical information systems, which if disrupted, compromised or destroyed partially or entirely may result in serious impact on the stability, security, economy, public safety, public health and/or essential public services of the Hong Kong Special Administrative Region, their data centre service providers should consult relevant data centre security consultancy, from early design stage for security advice on the security requirements and measures.

Site selection decision should be made after taking the above considerations into account and ascertaining the risks that are at an acceptable level or can be mitigated to an acceptable level.

5.6. Perimeter Level Security Design Considerations

Perimeter level defence is the first level defence of the data centre. While the actual security design would vary very differently depending on the site environment, the following common security design considerations for perimeter level defence should be taken into account:

a) High wall, fence and manned entrance door, vehicle gate with sufficient height, strength and anti-climb measures (e.g. mesh, spike, razor) should be built / set up to withstand possible intrusion, attacks or accidents like car crash and explosion;
b) Access Control System ("ACS") shall be set up for resident staff, pre-registered visitors and vehicles;
c) Entrances to the data centre should be kept to minimum;
d) Windows / glass curtains / glass doors / open areas should be avoided;
e) Closed Circuit Television ("CCTV") recording system with low-lux or infrared, motion detection cameras, covering all perimeter areas with no blind spot and resilient design should be installed, and integrated with the monitoring system to alert the security management team immediately on any intrusion or failure attempts into perimeter zone;
f) Radar-based or laser-based detection system should be installed to accurately detect intruders entering the data centre perimeter;
g) Vibration detectors should be installed to detect intrusion by boring holes;
h) Glass breaking sensors should be installed to detect intrusion by breaking windows, glass curtains or glass doors;
i) Depending on operational needs and availability of any nearby refuse collection point, dumping refuse to the refuse collection point near the premises should be considered to avoid refuse collection vehicles to go into the data centre;
j) Data centre, be it an *en bloc* building type or floor type, should be kept in a low profile on its appearance. There should be no signage to show that it is a data centre. The building name

should not show that it is a data centre, and the best efforts should be made to avoid the data centre being mentioned in social media and in the public domain, as far as possible;

k) Any general office area(s) should be at or outside the site perimeter; and

l) Floodlights with motion detection and public address system should be installed in high risk perimeter areas to deter intruders.

5.7. Clearance Zone Level Security Design Considerations

Clearance Zone level is the second level of manned defence of the data centre where visitors and their belongings or equipment as well as vehicles are checked. The following common security design considerations for Clearance Zone level defence should be taken into account:

a) Visitors' identities and their vehicles shall be checked against approved pre-registration records; admission of *ad hoc* visitors shall be approved by an authorised person with sufficient justifications; the entrance and exit of all persons and vehicles shall be logged, kept and properly maintained for audit purposes;

b) When conditions warrant, visitor parking area should be at location where is distant from the data centre;

c) For *en bloc* data centres, unregistered / unscreened vehicle shall not be allowed to enter the building where the data centre is situated;

d) The vehicular access should adopt the following security measures when conditions warrant:

   (i) double-layer / double-gate design;

   (ii) retractable bollards / road blockers;

   (iii) drop bar with lower and upper skirt; and

   (iv) intercom with CCTV coverage;

e) IT equipment brought into / out from the data centre shall be registered and approved by authorised persons;

f) No bag or container should be brought into the data centre. When it is necessary, the bag or container should be thoroughly screened before entry. Only items or equipment that are commensurate with the approved purpose for entering the data centre could be brought along with as "bring-in" items. After the activity is completed, all "bring-in" items shall be cleared and removed from the data centre;

g) Equipment not to be brought in data centre should be kept in the locker in Clearance Zone;

h) Clearance Zone should have handheld detector for detecting weapons like firearms and explosives;

i) When conditions warrant, sufficient space should be reserved in Clearance Zone to set up a walk-through metal detector and/or an X-ray machine. Additionally, a designated vehicle checking area, preferably outside the building, should be considered. This arrangement allows for tighter security checking if there is an escalation of the risk level, under which all resident staff and visitors and their belongings as well as all vehicles shall be checked thoroughly, in case the situation warrants;

j) A security control room should be manned round the clock. For those which are not manned 24 hours a day, remote monitoring ability should be equipped such as a remote alert system;

k) ACS with Multi-Factor Authentication ("MFA") should be set up for resident staff, pre-registered or approved *ad hoc* visitors;

l) Panic alarm system should be installed to quickly summon assistance from external security service providers in case of an emergency;

m) Authorised pathways going into other floors of the data centre should be kept to minimum, and entrance doors should be strong enough such as adopting inter-locking system; and

n) CCTV recording system should be installed covering all areas in the clearance zone.

5.8. Floor Level Security Design Considerations

Within each floor of a data centre, space is used for hosting IT equipment (i.e. **Data Hall Zone**) and supporting facilities such as power / cooling / fire suppression equipment and control systems (i.e.

Plant Area Zone), data centre office area zone and ancillary function area zone. Individual room within each zone is a sub-zone. The following common security design considerations for floor level defence should be taken into account:

a) Staff and visitors shall be assigned access rights to zones and sub-zones in the ACS according to their approved application for access;
b) Entrance to zones and sub-zones should be controlled using MFA. Depending on the security and operational needs, such as head counting function with due consideration on the need of emergency evacuation, exit to zone and sub-zone may also be controlled by MFA, single factor authentication, or even no authentication (fail-safe door lock[1] or fail-secure[2] door lock with manual release button);
c) CCTV recording system should be installed covering all areas in the floor level;
d) Data centre office areas or command centres should be restricted to specific data centre support staff who have an **inevitable onsite** operational need for access. Any other data centre support staff should be resided in general office areas at or outside the site perimeter; and
e) For floor level data centres, floor level is the first level defence of the data centre and all the security design considerations for the Perimeter and Clearance Zone levels are also applicable.

5.9. Plant Area Zone Security Design Considerations

The following common security design considerations for Plant Area Zone level defence should be taken into account:

[1] Fail-safe door lock, the lock will be released when power supply is lost or in the event of fire alerts

[2] Fail-secure door lock, the lock will be locked when power supply is lost or in the event of fire alerts

a) Staff and visitors shall be assigned access rights to plant area zones and sub-zones in the ACS according to their approved application for access;
b) Entrance to plant area zones and sub-zones should be controlled using MFA. Depending on the security and operational needs, such as head counting function with due consideration on the need of emergency evacuation, exit to zone and sub-zone may also be controlled by MFA, single factor authentication, or even no authentication (fail-safe door lock or fail-secure door lock with manual release button); and
c) CCTV recording system should be installed covering the whole plant area zone.

5.10. Data Hall Zone Security Design Considerations

The following common security design considerations for Data Hall Zone level defence should be taken into account:

a) Staff and visitors shall be assigned access rights to data hall zones and sub-zones in the ACS according to their approved application for access;
b) Entrance to data hall zones and sub-zones should be controlled using MFA. Depending on the security and operational needs, such as head counting function with due consideration on the need of emergency evacuation, exit to zone and sub-zone may also be controlled by MFA, single factor authentication, or even no authentication (fail-safe door lock or fail-secure door lock with manual release button);
c) CCTV recording system with motion detection cameras, covering the whole data hall zone with no blind spot and resilient design should be installed, and integrated with the monitoring system to alert the security management team immediately on any intrusion or failure attempts;
d) Data hall zone shall be designed and constructed in accordance with security needs;
e) Data hall zone should be built or renovated without windows to

avoid the risk of break-in and waste of energy;

f) Data cables should be protected in trunks and the part of trunks running through common areas should be locked;

g) Movement of goods and personnel to and from data hall zone should be controlled by appropriate door control mechanisms (e.g. interlocks, mantrap, anti-passback and anti-piggyback door controls);

h) Meet-Me-Room ("MMR") should be in place for IT systems to connect to telecommunications services. When conditions warrant, MMR should be built outside the data hall zone, and all the security design considerations for the Data Hall Zone levels are applicable to MMR. Carriers' equipment should be demarcated in MMR to minimise external parties accessing the data hall; and

i) Dedicated trunk should be used for data cables of dedicated security systems (e.g. ACS and CCTV recording system) when conditions warrant.

5.11. Aisle Level Security Design Considerations

An aisle is a sub-zone of the data hall zone. Usually, aisle doors are implemented for cold-aisle containment or hot-aisle containment purposes. Implementing access control at the aisle door level provides one extra level of access control to reduce the risk of unauthorised access to IT equipment. The following common security design considerations for Aisle level defence should be taken into account:

a) Staff and visitors should be assigned access rights to individual aisle(s) of the data hall zone in the ACS according to their approved application for access;

b) Entrances to aisles should be controlled using MFA. Depending on the security and operational needs, such as head counting function with due consideration on the need of emergency evacuation, exit to aisle may also be controlled by MFA, single factor authentication, or even no authentication (fail-safe door lock or fail-secure door lock with manual release button); and

c) CCTV recording system should be installed covering the whole of each aisle sub-zone. If CCTV at rack level is not implemented, aisle level CCTV monitoring is the last defence to deter and detect unauthorised access or access attempts to IT equipment racks.

5.12. Rack Level Security Design Considerations

Rack level defence is the last level of protection for the IT equipment inside the data centre. The following common security design considerations for rack level defence should be taken into account:

a) Staff and visitors shall be assigned access rights to individual equipment rack(s) of the data hall zone in the ACS according to their approved application for access;

b) Depending on the security needs, such as the criticality of the IT equipment, key locks with high-security features, such as resistance against picking, bumping, or unauthorised duplication of keys, should be installed on equipment racks;

c) Implementation of Smart Rack Door system should be considered as the rack door unlocking and locking can be integrated with ACS to accurately control, monitor and log the access to racks. For rack level security without implementing smart rack door system, access to rack doors should be controlled by physical locks, and the keys should be held by authorised persons only though such arrangement for large data centres would be manpower effort intensive and less efficient; and

d) When conditions warrant, the CCTV recording system should be set up to cover at rack level for providing accurate evidence of persons and time of access to the racks, however, the angle of CCTV cameras should be installed to avoid recording any keyboard input and monitor screens to mitigate the risk of leaking passwords of privileged accounts and/or restricted information displayed on monitor screens.

5.13. Operational Technology and Cyber-Physical System Security Design Considerations

Operational Technology ("OT") means hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in asset-centric enterprises, particularly in production and operations[3]. Examples of OT include: road blocker, drop arm and gondola system, etc.

Cyber Physical System ("CPS") means engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). When secured, they enable safe, real-time, secure, reliable, resilient and adaptable performance[4].

Examples of CPS include: Building Management System that controls heating, ventilation and air conditioning ("HVAC"), chillers and fans; automatic chemical dosing system for chiller water and concierge robot, etc.

OT and CPS are also adopting technologies of IT systems such as IP networking and general-purpose operating systems like Windows and Linux, which cause them no longer islands immune from cybersecurity threats and attacks. As a result, the traditional belief that OT and CPS are only subject to physical attack is no longer true. Incidents and impacts now occur along the entire cyber to physical spectrum. Since data centres usually deploy many OT and CPS, the following common security design considerations to address OT and CPS risks which are applicable to OT and CPS installed in data centres should be taken into account:

[3] Source : Gartner, Gartner Glossary, https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

[4] Source : Gartner, Cyber-Physical Systems - Gartner Definition, When Worlds Collide, Converge, and Evolve: IT Security, OT Security and the Rise of Cyber-Physical Systems Security, Katell Thielemann, 2020

a) Existing IT security management system, including intelligence collection, threat management and incident response approaches, should be extended to address the broader IT-OT cyber-physical security threat surface[5];
b) OT products that provide ongoing software security patch services, if available, should be selected, and testing environment of OT products patches should be set up. Alternatively, procuring supplier services to test and install software patches should be explored and chosen as far as possible; and
c) OT and CPS should be positioned deeper in the network architecture of the data centre for the purpose of implementing protective measures according to the defence-in-depth strategy against threats and attacks from external network.

[5] Source: Global Cybersecurity Alliance, Applying ISO/IEC 27001/2 and the ISA/IEC 62443 Series for Operational Technology Environments, July 2021

6. Data Centre Security Operational Practices

Data centre service providers shall apply core security principles and best practices concerning the issue of checks and balances in data centre security management. Data centre security management shall be considered in all stages from design, build and ongoing operation of the data centres.

The following elements of data centre security operational practices shall be considered:

a) Security Policies
b) Human Resources
c) Asset Management
d) Access Control (space and system)
e) Physical and Environmental Security
f) Operations Security
g) Security Incident Management
h) Service Availability and Continuity Management
i) Compliance

This Practice Guide should be read in conjunction with the prevailing Baseline IT Security Policy [S17], IT Security Guidelines [G3] and relevant procedures, where applicable, for applying any security practices also relevant to data centres and the associated IT infrastructures and systems.

6.1. Security Policies

Data centre service providers shall define and enforce their data centre security policies to provide management direction and support for protecting data centres and assets in accordance with the business needs and security requirements.

Data centre service providers shall promulgate their own data centre security policy. A mechanism for the delivery of the policy shall be established to ensure ease of accessibility and availability to all staff, functional groups and management.

6.2. Human Resources

Data centre service providers shall ensure that staff involved in data centre operations are competent in their roles, understand their responsibilities, and are aware of data centre security risks. This process shall be maintained throughout the entire employment cycle from new recruitment and change of post to termination.

6.2.1. Competencies

Data centre service providers shall ensure that sufficiently qualified personnel are in place and who have received the appropriate training with regular assessment to manage the proper operations of data centre facilities and infrastructures in support of operational needs.

6.2.2. Security Awareness Training

Data centre service providers shall organise security awareness training for their support staff regularly or as needed. The training should at least cover guidelines on the following items:

a) Misbehaviour (e.g. tailgating and piggybacking);
b) Suspicious activities (e.g. loitering, leaving articles unattended);
c) Malicious activities (e.g. air espionage by drones); and
d) The latest illegal activities.

Data centre support staff shall also be reminded to stay vigilant at all times and to question any suspicious visitors or any suspicious acts of the visitors in the data centre.

6.2.3. Security Vetting

Besides resident staff working and supporting the data centre operations, there are visitors, like contractors of clients/data centre service providers, requiring to enter the data centre day-to-day for performing relevant IT systems support activities, such as delivery of equipment, maintenance of IT systems, etc. These staff and visitors can even get full physical control of IT equipment and data of their authorised systems in the data centre, and hence personnel security risk is always imminent. To address human related risks, the following common security considerations should be taken into account:

a) Staff and visitors shall be assigned access rights to the floor, zone (e.g. data hall), sub-zone (e.g. room or aisle) and IT equipment racks in data centre in the ACS according to their approved application for access, and MFA should be used for securing the access only by authorised persons; and
b) Support staff working in the data centre including visitors such as contractors should either pass the relevant and applicable security check processes (e.g. criminal record check, background verification checks, if considered necessary) or be under surveillance or escort.

6.3. Asset Management

Data centre service providers shall maintain appropriate protection of all the hardware, software and data assets being hosted in the data centre.

6.3.1. Inventory of Assets

An inventory of assets helps ensure that effective protection of assets and identification of lost assets could be taken place. Periodic review of the inventory shall be conducted to ensure that the assets are properly owned, kept and maintained.

6.3.2. Asset Ownership

Asset ownership shall be assigned or identified when assets are created or transferred from other parties. The asset owner is responsible for proper asset management to ensure that the assets are inventoried, appropriately protected, properly handled for their disposal or reuse. Additionally, access restrictions to assets should be defined and reviewed periodically by the asset owner.

6.4. Access Control (Space and System)

Data centre service providers shall restrict access to the spaces (areas) and systems of the data centre based on the inevitable necessary operative minimum. This pertains to the aspects of **areas**, **time**, **personnel** and **knowledge**.

6.4.1. Principle of Least Privilege

Data centre service providers shall ensure that the least privilege principle is followed when authorising privileges to access the areas and systems of data centres. In other words, personnel shall only have access to what they absolutely need in order to perform their duties and no more. The principle aims to minimise the attack surface, and to enhance the protection from faults and malicious behaviour.

6.4.2. Access Control with Coloured Wearable

Personnel wearing coloured wearables for different authorised zones or sub-zones within the data centre should be adopted to easily and quickly identify different types of staff or visitors for their authorised access areas.

6.5. Physical and Environmental Security

Data centre service providers shall uphold the physical security of their data centres to prevent unauthorised physical access, damage, theft or compromise of assets, and interruption to data centre services.

6.5.1. Security Systems Segregation Design

When conditions warrant, the servers used for security systems should be completely segregated from non-security related systems, including their trunks and conduits. This separation helps contain access to security systems by authorised security system related personnel only.

Additionally, a testing environment for security systems should be established to evaluate patches before applying them in the production environment.

6.5.2. Data Centre Physical Security Design

In addition to the data centre security design considerations specified in Section 5, the following considerations for security installation features should be duly taken into account to support ongoing data centre operation.

6.5.2.1. Roller Shutter / Metal Gate

Roller shutter / metal gate should be equipped with ground lock, and the control panel should be placed in the secured side.

6.5.2.2. Access Door

To strengthen security, manual release buttons on doors should be avoided and replaced with an authorisation system such as a card reader.

For access to security areas, a metal door should be used. All magnetic locks of door should be placed in the secured side. To minimise the risk of break-ins, windows on doors should be minimised or secured with steel bars or metal mesh.

6.5.2.3. Intruder Detection System

Intruder Detection System (IDS) should be installed to include the following features / functions:

a) CCTV video analytics capability should be employed and integrated with IDS;
b) Intrusion prevention features should be enabled for the perimeter, alley, public facing and low-level windows / doors, emergency access and critical facilities;
c) Glass break / vibration / motion / infrared / LiDAR sensors, alarmed push-bars and also contact alarms should be installed at appropriate locations; and
d) Active intrusion monitoring system with alert messages should be enabled.

6.5.2.4. Public Address / Display System

Public address / display system should be provided with the following features:

a) Disseminating floor / area / zone specific information / messages;
b) Pre-recording alerts / warnings for security / emergency situations; and
c) Preventing unauthorised tampering.

6.5.2.5. CCTV Recording System

When conditions warrant, the CCTV recording system should have video analytic ability to form an integral part of the whole security framework of data centre. The CCTV coverage should cover every part of the data centre.

The technical / functional specifications for CCTV recording system should include the following features:

a) At least 2K resolution;
b) Minimum 30-day retention with automatic fallback / backup storage;
c) Supported by dual power sources and UPS with emergency power backup;
d) Night vision;
e) Motion detection;
f) Resilient design to eliminate single point of failure;
g) Full coverage with no blind spot;
h) All spots to be covered by at least 2 cameras to eliminate single point of failure and to avoid blockage of vision due to object movement; and
i) Integrated with the monitoring system to alert security personnel immediately with visual and audio pop-up alarm on any intrusion or failure attempts.

Video signal should be repeated to another security control room / operation room for live monitoring and instant response.

6.5.3. Physical Access Control

All access keys, cards, passwords, etc. for entry to any data centre facilities, infrastructures, operation supporting systems and networks, shall be physically secured, subject to well-defined and strictly enforced security procedures.

6.5.4. Fire Exit Access

All fire exit access should be equipped with multi-point push bars or break glass unit with Intruder Detection System (such as contact sensors) and local buzzer covered by CCTV. Also, depending on the circumstance allowed after risk assessment, time delay circuit (e.g. allowing 15 or 30 seconds delay to ascertain nature of incident) could be adopted in fire exit access / escape to ensure security.

6.5.5. Stringent Security Controls for High Protection Class Data Centre Spaces

Stringent security controls shall be introduced for high protection class data centre spaces such as Hardware Security Module ("HSM") rooms, Telecommunications and Broadcasting Equipment ("TBE") rooms and Meet-Me-Rooms ("MMRs"), etc.

Dual control biometric locks with proper audit mechanism should be considered for access to HSM rooms.

Access to TBE Rooms and MMR by carriers' staff shall be under full escort by authorised data centre support staff. Other personnel without **inevitable** operational needs are restrictly prohibited to enter TBE or MMR.

6.5.6. Fire Risks and Fire Fighting

The data centre spaces shall be considered as different fire compartments each with their own fire detection, alarms and suppression objectives.

Fire-stopping techniques such as the use of fire-rated materials, construction details, the orientation of the fire compartment structure, etc., should be duly considered when applied to pathways that go through the boundary of fire compartments.

A fire-fighting party of the data centre should be organised in each operating shift with well-defined responsibilities assigned to each officer in concern. Regular fire drills shall be carried out to allow the officers to practise the routines to be followed when a fire breaks out.

Other support staff not being members of the fire-fighting party shall be taught how to operate the fire detection, prevention and suppression system and the portable fire extinguishers.

No unauthorised storage of hazardous, flammable or combustible materials within data centres.

6.5.7. No Photograph or Video Recording

Unless authorised by data centre management, taking photographs or video recordings shall not be allowed within data centres to avoid potential exposure of sensitive information, such as data centre equipment model and security measures.

6.5.8. Preparedness for Extreme Weather Conditions

Data centre service providers should not only identify potential risks and vulnerabilities related to extreme weather, such as flooding, lighting strike, and landslide, but also explore preventive measures, such as regularly checking drainage systems, to ensure no blockages that may impede water flow, and install water leakage and power supply monitoring system for active monitoring.

An emergency response plan should be formulated for extreme weather conditions. The plan should outline detailed actions to be taken before, during and after extreme weather events. The plan may also encompass elements for weather monitoring, protocols for communication and reporting, evacuation plans and contingency arrangements to ensure a prompt and effective response.

6.5.9. No Signage Indicating the Location of Critical Room / Area

To ensure the protection of power, signals, switches, cables, TBE and HSM, unless required by statute (e.g. Code of Practice for the Electricity (Wiring) Regulations), there should be no signage indicating the location of the critical rooms / areas housing aforementioned equipment.

6.6. Operations Security

6.6.1. Operational and Administrative Procedures

Operational and administrative procedures (e.g. Standard Operating Procedures (“SOPs”), Methods of Procedures (“MOPs”) and Emergency Operating Procedures (“EOPs”) for data centre facilities and infrastructures) shall be properly documented, followed, maintained and reviewed regularly and made available to staff who need them.

6.6.2. Dual Control for Key Operations

Dual control measure, which involves two authorised individuals for key operations (e.g. access to HSM), should be implemented to minimise the risk of errors, fraud or malicious activities.

6.6.3. Regular Job Rotation

Regular job rotation for data centre support staff, in particular supervisory officers, should be adopted as far as possible to help uncover misdeeds, discover previously overlooked discrepancies, reduce insider threats, and enhance skills and knowledge of backup staff.

6.6.4. Change Management

Changes affecting existing security protection mechanism shall be carefully considered. Changes to data centre facilities and infrastructures affecting or potentially affecting data centre service level shall be subject to strict change management control, and the following requirements / procedures should be taken into account:

- Identification and recording of significant changes;
- Planning and testing of changes;

- Assessment of the potential impacts, including security impacts;
- Formal approval procedure for proposed changes;
- Communication of change details to all relevant parties;
- Fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events; and
- Provision of an emergency change process to enable quick and controlled implementation of changes for resolving an incident.

6.6.5. Permit-to-Work

Only authorised works / activities shall be allowed inside the data centre. A Permit-to-Work shall be obtained from the data centre management prior to any works to be performed within the data centre in order to have proper management on any works as they may affect data centre service availability. Risk assessment with necessary mitigation and contingency measures shall be in place to ensure the data centre service availability.

6.6.6. Capacity Management

The use of resources should be monitored for capacity management. Capacity requirements should be identified according to the business requirements of the concerned data centre service components (e.g. CCTV recording system, ACS, etc.).

6.6.7. Prevent, Detect, Respond and Recover

Regular review of CCTV footages should be enforced to detect possible indicators of unauthorised access, intrusion, reconnaissance or trespassing activities.

Data centre service providers shall determine the retention period of personal data collected (e.g. any personal identifiers or the video footage recorded by CCTV) according to their security and operational needs, and destroy the personal data collected once the purpose of collection is fulfilled, to comply with the requirements under the Personal Data (Privacy) Ordinance (PD(P)O). The minimum retention period should be at least 30 days[6].

Whenever possible, data centre service providers should consider the use of video analytics to provide instant video footage analysis, including facial recognition, motion detection, abandoned object detection and behavioural recognition, among others, to improve the effectiveness of their surveillance operations.

Regular physical intrusion response drill should be conducted to ensure the preparedness and awareness of relevant data centre security management staff in response to physical intrusion. Sufficient training should be provided to data centre security management staff for prevention, detection, response and recovery measures and procedures to properly handle physical security of data centres.

Whenever necessary, physical penetration tests should be considered to identify vulnerabilities and evaluate existing physical security measures and controls of a data centre in response to the latest security landscape.

6.7. Security Incident Management

Data centre service providers shall ensure a consistent and effective approach to the management of data centre security incidents by conducting regular security drills and exercises, formulating and reviewing an emergency response plan, including a mechanism on reporting the security incident to necessary parties within a specified time frame depending on the seriousness of the incident.

[6] Source: Source: Section 13.1 (c) of the IT Security Guidelines [G3]

6.7.1. Incident Monitoring and Detection

A sufficient level of security measures for incident monitoring and detection shall be implemented to protect the data centre during normal operation as well as to monitor potential security incidents.

6.7.2. Security Incident Reporting

A reporting procedure shall be established and documented to clearly define the steps and processes in reporting any suspicious activities to all parties involved in a timely manner. Comprehensive contact information, such as telephone numbers (office hours, non-office hours and mobile), email addresses and fax numbers, should be set out in the reporting procedure to ensure effective communication among responsible personnel.

6.7.3. Security Incident Response

Proper and advanced planning can ensure that the incident response activities are known, co-ordinated and systematically carried out. It also facilitates the data centre service provider to make appropriate and effective decisions in tackling security incidents and, in turn, minimises the possible damages.

A security incident response plan shall be established and documented. Regular review for security incident response plan shall be conducted at least once every two years[7], or when there is any material change in the operating environment of the data centre. Data centre service providers shall ensure that all relevant personnel are familiar with the plan, and the plan should be made known to all staff, including management personnel, for their reference and compliance. Data centre service providers shall conduct drills at least once every two years[7], preferably annually, to assess the

[7] Source: Section 18.1 (c) of the IT Security Guidelines [G3]

effectiveness of the plan. The incident response team members shall participate in the drills to familiarise themselves with their roles in the incident response plan to ensure quick and effective response to security incidents.

6.7.4. Disclosure of Information about the Incident

Staff shall not disclose information about the data centre, individuals or specific facilities and infrastructures that have suffered from damages caused by crimes and abuses or the specific methods used to exploit certain vulnerabilities to any people other than those who are handling the incident and responsible for the security of such systems or authorised investigators involving in the investigation of the crime or abuse.

Any disclosure of information about incidents, including how to compromise and the background of the data centre, such as physical location, may encourage intruders to intrude on other data centres with similar vulnerabilities. Moreover, the disclosure may affect the forensic and prosecution processes under Police investigation.

6.8. Service Availability and Continuity Management

6.8.1. Service Availability Management

To ensure the service availability, data centre service providers should implement effective operational measures, including, but not limited to:

a) Ensuring the availability of trained service personnel;
b) Storing of spare parts;
c) Establishing maintenance contracts and service level agreements; and
d) Establishing effective communications protocols and precise emergency procedures.

6.8.2. Continuity Management

Contingency planning refers to interim measures to recover services following an emergency or system disruption. Interim measures may include the relocation of services and operations to an alternate site, the recovery of services using alternate equipment, or the performance of services using manual methods. The contingency plan should be fully documented and regularly tested. Data centre service providers should also assess the security risks in the business continuity site or alternate work site to ensure that sufficient security controls are in place to protect the sensitive data.

There are different types of contingency plans for data centre services. The most common one is the Business Continuity Plan ("BCP"). BCP focuses on sustaining an organisation's critical business processes during and after a disruption. In BCP, data centre service providers from the business side should assess the criticality of the services concerned, conduct business impact assessments, identify recovery time objectives and recovery point objectives, and define minimum service levels. Regular drills and exercises for BCP should be conducted under all available fallback options.

6.8.3. Environmental, Social and Governance (ESG)

To ensure business continuity of data centres, data centre service providers are advised to observe and monitor the latest ESG development and requirements, including the adequate long-term supply of refrigerants and ensuring the long-term availability of maintenance service for fire suppression systems. Some relevant practice guide and developments, but not exhaustive, are listed below for reference:

a) Green Data Centres Practice Guide (https://www.beamsociety.org.hk/BEAM-Plus/BEAM-Plus-Data-Centres/Green-Data-Centres-Practice-Guide)
b) Carbon Neutrality and Sustainable Development (https://cnsd.gov.hk/en/)

6.9. Compliance

Data centre service providers shall avoid breaches of legal, statutory, regulatory or contractual obligations when implementing or operating security measures. Security measures shall be implemented and operated in accordance with the respective security requirements and compliance with the relevant legal and contractual requirements. The compliance requirements provided as listed below may not be exhaustive, but will be reviewed and updated regularly as when required.

6.9.1. Compliance with Legal and Contractual Requirements

To avoid breaches of legal and contractual requirements, data centre service providers shall explicitly identify, document and keep up-to-date with all relevant statutory, regulatory and contractual requirements applicable to the operations of their data centres and each information system, if applicable, hosting in their data centres. The specific controls and individual responsibilities to meet these requirements should be defined and documented. The security of data centres should be regularly reviewed. Such reviews should be performed against the appropriate security policies, and data centres should be audited for compliance with applicable security implementation standards and documented security controls.

Data centre service providers shall observe the guidelines developed by the Office of the Privacy Commissioner for Personal Data (“PCPD”), when handling personal data collected by their security installations, such as ACS, CCTV recording system, etc., including:

a) Guide To Data Protection by Design for ICT Systems (https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf)
b) Privacy Management Programme (https://www.pcpd.org.hk/pmp/pmp.html)
c) Guidance on CCTV Surveillance and Use of Drones

(https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_CCTV_Drones_e.pdf)

For better protection of cross-boundary data flow within the Greater Bay Area, data centre service providers or the relevant information system owners where appropriate shall observe and be compliant with the following requirements / laws / ordinances:

a) The compliance arrangement on conducting cross-boundary flow of personal information within the Greater Bay Area (https://www.digitalpolicy.gov.hk/en/our_work/digital_infrastructure/mainland/cross-boundary_data_flow/);
b) Cybersecurity Law of the People's Republic of China;
c) Data Security Law of the People's Republic of China;
d) Personal Information Protection Law of the People's Republic of China; and
e) Personal Data (Privacy) Ordinance of the Hong Kong.

For data centres hosting information systems that handle payment card transaction and data, data centre service providers or the relevant information system owners where appropriate shall observe applicable requirements of the Payment Card Industry Data Security Standards ("PCI DSS").

- END -