HITACHI

INSPIRE THE NEXT

INFORMATION SECURITY REPORT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Even if the vast amount of diverse data in modern society has many positive effects, there are also big security and safety dangers. A substantial change in work practises, such as the encouragement of working from home, and a significant change in how security will be given in the future have both been brought on by the present COVID-19 outbreak. Security threats are more specialised, intricate, and diverse than ever, and current attack approaches are being merged more and more frequently. Therefore, the main objective of this study is to develop a security programme to improve the information security of the Hitachi Ltd organisation. This paper provides information regarding information security. In relation to information security, it provides an overview of Hitachi's policy, frameworks, guidelines, management cycle, risk assessment management and other issues.

COMPANY BACKGROUND

Hitachi ltd is a Japanese multinational business has its headquarters in Chiyoda, Tokyo. It belongs to the DKB group of enterprises and is the parent firm of the Hitachi group. Hiitachi ltd is a very diversified firm, it runs eleven different business sectors such as Information and telecommunication systems, Social infrastructure , high functional materials and components, financial services, railway and urban systems, digital media and consumer products, construction machinery and other components and systems. (pandey, 2017)

Under these circumstances like Russia-Ukraine war, covid -19 epidemic ,Hitachi were able to achieve an adjusted operating income ratio of 7.2% in fiscal 2021.Hitachi is a member of the Nikkei 225 and TOPIX indices and is listed on the Tokyo Stock Exchange. It is placed **129**th in the 2012 Forbes Global 2000 and **38**th in the Fortune Global 500 for 2012. The cloud storage company Backblaze published statistics on January 21, 2014, stating that Hitachi hard discs are the most dependable among well-known hard disc manufacturers. (CEO Message : Investor Relations : Hitachi Global, n.d.)

Capital	-	461,731 million yen
Number of employees	-	29,485
Consolidated number of employees	-	368,247
Net sales	-	1623424 million yen
Consolidated revenues	-	10,264,602 million yen
Licenses	-	ISO9001/IEC20000/27001
		Privacy mark, COPC CSP standard
Representative	-	Keiji Kojima Director, Representative Executive Officer, President & CEO

Main objectives

- Accelerating customer innovations with advanced IT solutions.
- Contribute to a stable energy supply for customers and the realization of low carbon and decarbonized society.
- Providing people with safe, secure, and comfortable transportation with railway system.
- Designing smart cities to be more convenient and environmentally friendly.
- Providing advanced sustainable technologies for mobility to the automotive and motorcycle industries. (Hitachi ltd, 2022)

DATA RELEVANCE TO COMPANY

According to Hitachi group, Data may power innovation and drive corporate change, but without rigorous management and regulation of data collecting, it may not live up to its potential. Using the three V's as a framework, Hitachi ltd can describe the properties of big data. The volume of data being stored is growing exponentially. This data is available in a wide variety of structured and unstructured formats. Additionally, data velocity is influenced by how quickly information must be gathered, processed, and retrieved in addition to how quickly it flows. Big Data is expected to help Hitachi ltd better comprehend what their customers are thinking. The capacity to forecast what the consumer wants and how to reach her could be improved through more targeted business analytics as a result of this. (Harry E. Pence, 2014)

Every day, 2.5 quintillion bytes of data are produced. Through a multi-cloud and hybrid strategy, more than 50% of data are moving to the cloud, with the remaining staying on-premises. This method has a significant influence on cost savings, customer satisfaction, revenue, and business value.

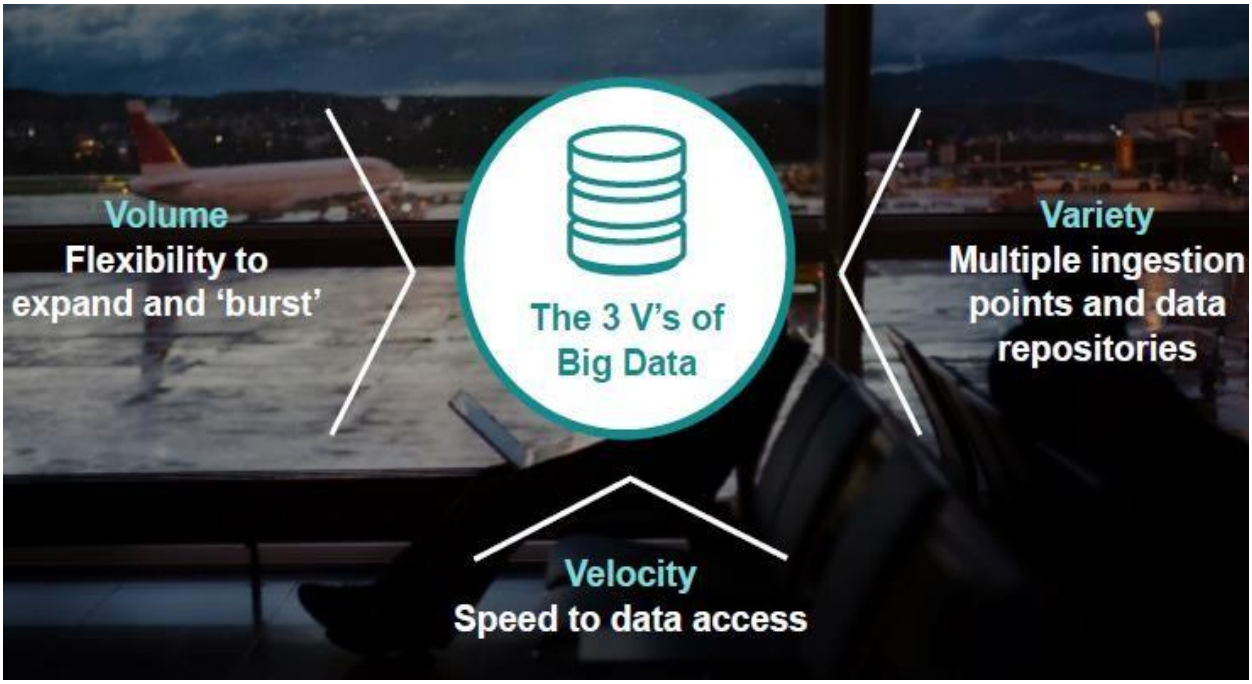


Figure 1: V's of big data

Hitachi ltd performs a defined set of activities

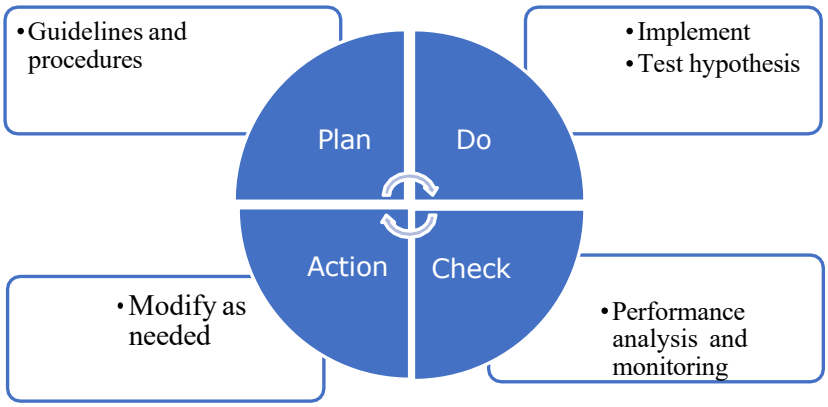
- Setting measurable goals for the use cases of clickstream analytics, device or equipment log analytics, and social sentiment analysis.
- Specify pertinent sources for the following data types: click stream data, in memory analytics, real-time streaming, data warehousing and legacy data (RDBMS).
- Chosen preferred data visualisation tool
- Create dashboards and reports for each use case.
- Review the big data solution's current financial model. (Hitachi Data System, 2022)

Analytics, integration, intelligence, and big data solutions are the main areas of concentration for Hitachi Data Systems. These basics consist of

- the capacity to mix structured and unstructured data,
- the capacity to manage data as it scales in real time,
- the capacity to analyse data to generate insightful knowledge, and
- the capacity to correlate data from many sources. (Hitachi ltd, 2020)

INFORMATION SECURITY FRAMEWORK

The PDCA (Plan-Do-Check-Action) cycle is used by Hitachi to manage information security, which includes managing personal information. Hitachi creates guidelines and procedures for information security management during the Plan phase of the PDCA cycle. Hitachi puts these guidelines and precautions into effect in the Do stage. Raising awareness of and monitoring action in the Do stage is part of the Check stage, which leads to the Action stage, where continual improvements are achieved. The entire cycle takes six months to complete. (Hitachi, 2021)



Based on the three concepts of "Governance," "Co-creating security," and “taking responsibility” for a "new normal" society, Hitachi is now advocating a number of programmes to increase cyber resilience. (Hitachi, 2021)

GOVERNANCE

- Continue and systematically deploy security precautions that have made governing cyber security a management concern. Since there is no such thing as total security, we must increase our capacity for resilience to enable quick recovery in emergency situations.

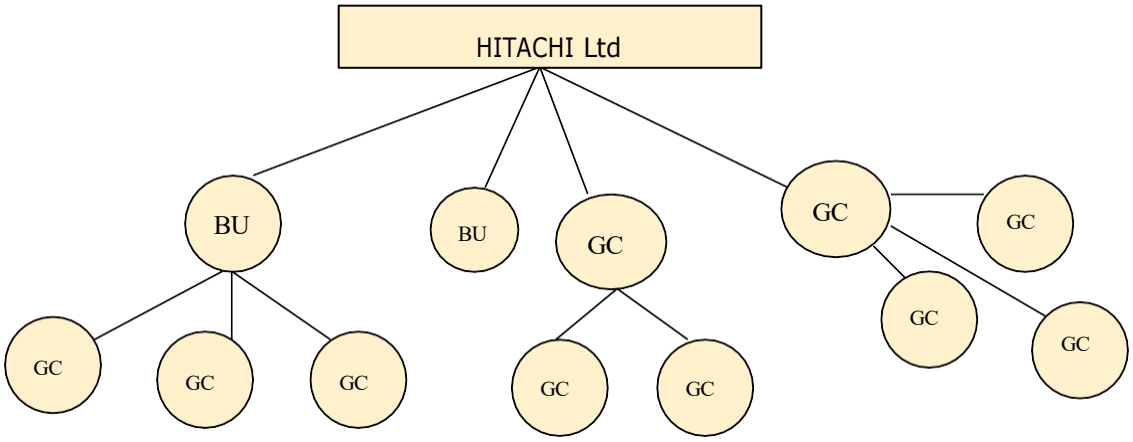
CO-CREATING SECURITY

- To defend against the changing and growing cyberattacks, society as a whole must improve internal communication and create a security ecosystem.

TAKING RESPONSIBILITY

- Each employee gains a thorough awareness of security, recognises its significance, and develops the responsibility taken mentality of acting on one's own behalf.

MINDMAP



HITACHI Ltd

CEO

Chief information security officer(CISO)

Information security audit officer

Information security committee

Information security promotion

Business unit (BU) office

Information security(IS) officer

- Information security promotion division
- Person responsible for implementing
- Information security
- External liaison division
- Cybersecurity officer
- Information system manager
- Information system manager

Chief Information security audit officer

Group company (GC)

Company president

- IS officer
- Audit officer

Integrating fully developed IT security mechanisms include encryption, access control systems, ID management and filtering

Collecting and Analyzing Threat Information, and Disseminating Vigilance Information

A chief information security officer (CISO) and a chief information security auditor are both chosen by the president and CEO. The CISO is in charge of promoting information security and serves as head of the IS committee, which sets policies, educational programmes, and initiatives pertaining to information security. All Hitachi Group business sites and organisations are informed of his or her decisions, and each IS officer oversees their comprehensive implementation in the workplace. All departments at Hitachi undergo annual audits by the IS chief auditor regarding information security and the protection of personal information. To assure the fairness, impartiality, and independence of these audits, he or she conducts them independently. On a group-wide scale, Hitachi's conducts audits and inspections; group companies in Japan conduct audits comparable to those conducted at Hitachi, Ltd., which subsequently confirms their findings. A common worldwide self-check system is used by group companies abroad. (Hitachi ltd, 2020)

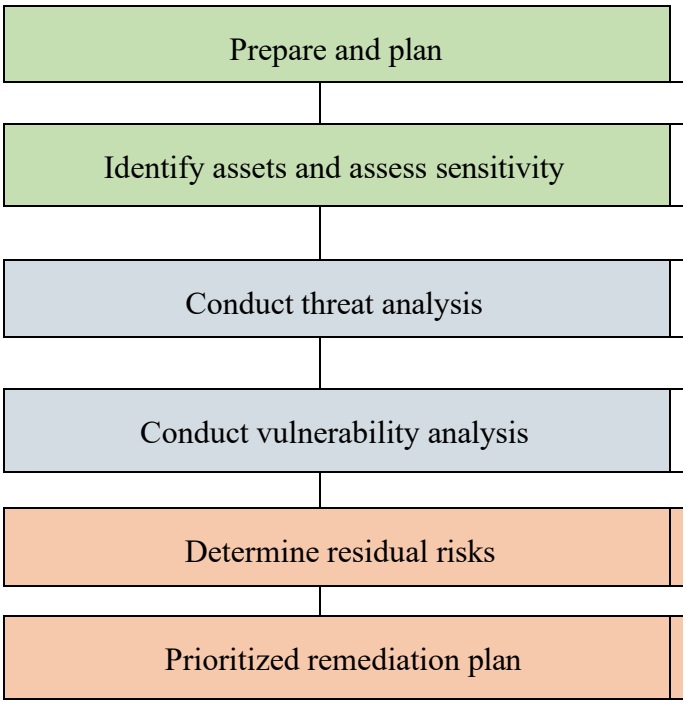
In an effort to stop information leaks, Hitachi is creating standardised IT security measures like encryption, a variety of access control systems, ID management, and filtering. We are enhancing a number of countermeasures, such as defence in depth controls, early detection techniques, and first reaction plans, to protect against cyberattacks. (Hitachi ltd, 2020)

RISK ASSESSMENT MANAGEMENT

In accordance with the international standard ISO/IEC 7001, which regulates the management of information security, Hitachi designed global information security administration standards. In order to improve overall IS management, Hitachi simultaneously promoting a continuing IS management system.

As cyberattack techniques become more varied, incidents are coming from a greater range of sources and having a wider range of effects. Hitachi has broadened the scope of its risk management efforts, which had traditionally concentrated on measures connected to internal IT environments, and is promoting cyber security and risk management activities as a response to hazards in these circumstances. (Hitachi ltd, 2020)

RISK MANAGEMENT APPROACH



In the prepare and plan stage, Our system's goals, boundaries, and system description have all been established. Its notion of operation has also been described. The qualities of confidentiality, integrity and availability are used to identify and evaluate assets in the second stage. The capability, motive, and likelihood of the threat agents are examined at as scenarios are built in conduct threat analysis. The many attack types that system assets are susceptible to are identified, and the resources and capabilities an agent needs to launch an assault are described in vulnerability analysis. Your IT system's operational risk is quantified; risk is a function of the

impact of threat scenarios and the possibility that they will materialise. Prioritized remediation plan undergoes to assist establishment of foundation for a comprehensive, successful risk mitigation approach, all detected risks are prioritised, and a final overall assessment is offered. (Hitachi ltd, 2020)

RISK ASSESSMENT

The critical tool used for risk assessment is TRA(Threat and risk assessment). It allows to understanding the numerous risks to your IT systems, assessing the amount of risk to which these systems are exposed, and suggesting the proper level of protection. To make sure organisation are not introducing new risks, they should do a TRA on the new components if adding new applications or systems to the environment, changing current information technology environment, or sharing information with new external entities. Since the threat landscape and environment's vulnerabilities are constantly changing, periodic TRAs on existing environments are necessary. (Jonny, 2019)

An investigation and interpretation of the threats existing in organisational and technical environment are provided by a threat and risk assessment. Using security and IT control frameworks like the Harmonized TRA Framework, ITIL, NIST, and the ISO 27000 series of IT security management best practises, Hitachi Systems Security Inc. has a thorough understanding of and competence in. The purpose of a TRA is to give the pertinent information that we need to make an educated decision about how to handle the risks that have been identified. (Hitachi system security inc, 2017)

TRA process

1. Request initiated
2. Develop assessment scope, plan and schedule
3. Conduct assessment
    - Review security plan, documentation, controls
    - Conduct vulnerability scans
    - Perform threat analysis(NIST 800-30 P12)
    - Identify risks
4. Risk mitigation and recommendations
5. Results and completion

The conduction of risk assessment on threats such as DDOS attack, accidental file deletion, system failure has shown on below table.

Threat	Vulnerability	Asset	Impact	Likelihood	Risk	Recommendation
High DDOS attack	Firewall is properly configured and has effective DDOS mitigation-high	Website - critical	Website resources will be unavailable - critical	DDOS was discovered once in 2 years-medium	Potential loss of $10,000 per hour of downtime-medium	Monitor the firewall
Accidental file deletions - High	Permissions are set up correctly, IT auditing software is in place, backups are taken regularly-High	Files on a file share-medium	Critical data could be lost but almost could be restored from backup.-low	Medium	Low	Continue monitoring permissions changes, privileged users and backups.
System failure-High	10 years old air conditioning system- High	Servers-critical	Services such as email, websites etc will be unavailable for atleast 3 hours-critical	Temperature in server room will be 40c-High	Potential loss of $ 50,000 per occurance -high	Buying a new air conditioner $3000 cost

Table 1: Risk assessment analysis(Hitachi system security inc, 2017)

HITACHI INCIDENT RESPONSE ACTIVITY

The HIRT's job is to continuously assist Hitachi's cybersecurity countermeasures through incident response, which involves avoiding and resolving cyberattacks, and vulnerability handling, which closes security gaps that threats may exploit. The team approaches these challenges from the angles of collaboration and intra-organizational activities. The goal of HIRT is to identify emerging dangers early and implement countermeasures like enhancing security monitoring, penetration testing, monitoring firewall etc as soon as feasible in order to contribute to the realisation of a safe and secure internet society. (Hitachi, 2021)

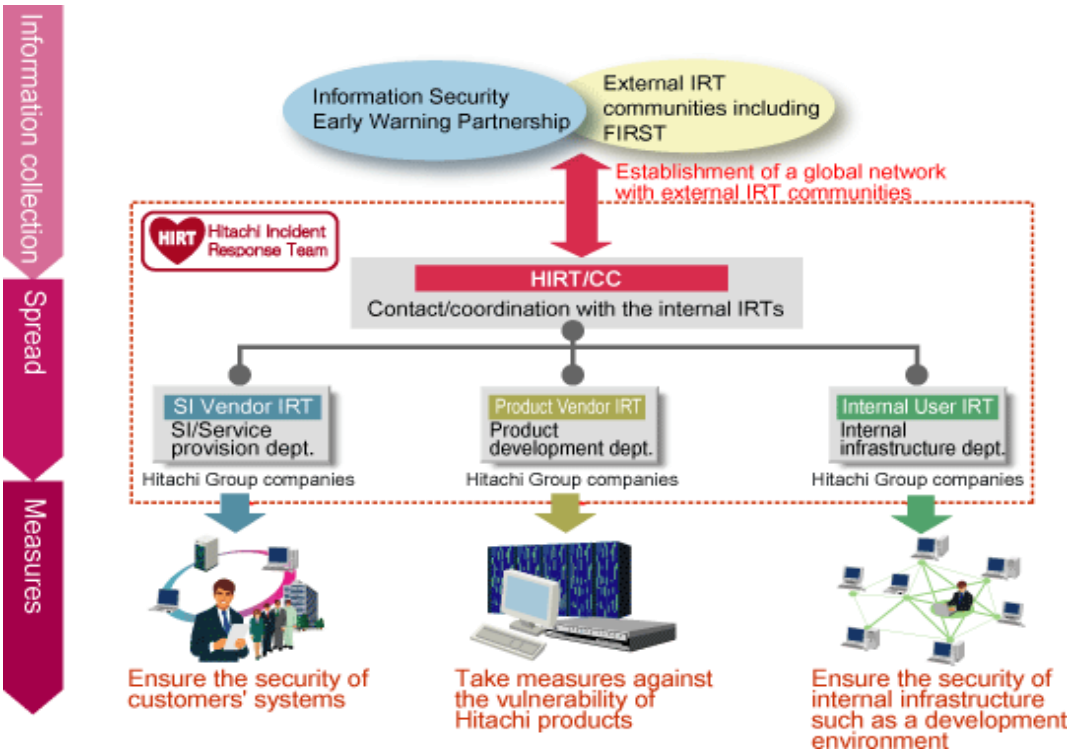


Figure 2: HIRT activities (Hitachi IR team, 2007)

Hitachi can set up a task force that manages the reaction at the corporate level if a threat could have a significant impact on business operations at several sites across the organisation or make it impossible for business to continue as usual. (Hitachi, 2021)

INFORMATION SECURITY POLICY

Since Hitachi is an organisation that helps to promote Japan's reputation on the international stage. Hitachi recognises that security risks are business risks and works hard to secure information security by developing a security policy that works with the larger management policy of the company.

- Creating administrative security rules and ensuring their development over time.

Hitachi will create administrative standards for information security that abide with the law and other regulations because it recognises that information security initiatives are a major concern for management and business operations. Additionally, Hitachi will create and oversee the implementation of a corporate-wide information security management structure with officials from Hitachi, Ltd. at its center. From an organisational, individual, physical, and technical standpoint, Hitachi will uphold information security and assure its ongoing progress.

- The continual preservation and management of information assets.

Hitachi employs safe management practises to effectively safeguard information assets from risks to their availability, confidentiality, and integrity. To ensure that company operations continue, Hitachi also puts in place the necessary control mechanisms.

- Legal and regulatory compliance.

Hitachi ensures that its administrative information security standards comply with all applicable laws and other regulations pertaining to information security. Hitachi takes the required corrective measures as outlined in the employee work rules and other pertinent regulations in the case of a legal or regulatory breach.

- Education and training.

Hitachi aims to improve information security awareness among its executives and workers and conduct education and training in relation to information security.

- Prevention of incidents and action taken.

Hitachi works to prevent information security events and, in the event that one does occur, to respond appropriately and promptly, taking steps to stop it from happening again.

- Ensuring that internal corporate group business processes are optimised

Below mentioned policy state that Hitachi will make an effort to create organisational structures that guarantee proper business procedures inside the corporate group made up of Hitachi and Hitachi Group entities. (Hitachi, 2021)

Email policy example:

The [COMPANY NAME] (the "Company") email policy is outlined in this document. This policy is a requirement for all workers who use the company's email system.

1. Business Use - The email system may only be used by Company workers for Company business and not for their personal use.

2. Ownership: The Company is the exclusive owner of any data and messages created, transmitted, received, or stored on the company's email system.

3. Email Review: The Company has the right to monitor, access, read, disclose, and otherwise make use of any and all emails.

4. Security : Only approved users are permitted to use the email system, and in order to access it, an employee must have received a password. Employees are forbidden from sharing their codes or passwords with anyone, and they are also forbidden from using someone else's code or password without the company's express written consent. (Email Policy Strict Template | Business-In-a-BoxTM, n.d.)

Password policy example:

Overview: A crucial component of computer security is passwords. They are the user accounts' first line of defence. The entire corporate network of the business could be compromised by a bad password. Therefore, it is everyone's responsibility to choose and secure their passwords by following the instructions in the following. This responsibility extends to contractors and vendors who have access to company systems.

Purpose : This policy's objective is to establish best practises for creating secure passwords, safeguarding them, and determining how frequently they should be changed.

General guidelines for constructing strong password:

contain at least one of each of the following

- digit (0..9)
- letter (a..Z)
- punctuation symbol (e.g.,!)
- control character (e.g., ^s, Ctrl-s) are based on a verse (e.g., passphrase) from an obscure work where the password is formed from the characters in the verse. (Password Policies, 2015)

REFERENCES

CEO Message : Investor Relations : Hitachi Global. (n.d.). Www.hitachi.com. https://www.hitachi.com/IR-e/corporate/message/index.html

Hitachi ltd. (2020). *Hitachi integrated report 2020*.

Hitachi ltd. (2022). *Business Information : Investor Relations : Hitachi Global*. Www.hitachi.com. https://www.hitachi.com/IR-e/corporate/business/index.html#8100205

Hitachi system security inc. (2017). *Hitachi-Systems-Security_Threat-and-Risk-Assessment*.

Jonny. (2019). *Cyber Security TRA (Threat and Risk Assessment) Resources Research*.

pandey, M. (2017). *Hitachi Marketing Research Report*.

Hitachi. (2021). *Information Security Report 2021*.

Email Policy Strict Template | Business-in-a-Box™. (n.d.). Www.business-In-a-Box.com. https://www.business-in-a-box.com/template/email-policy-strict-D710/

Password policies. (2015, June 15). Www.ibm.com. https://www.ibm.com/docs/en/spim/2.0.0?topic=administration-password-policies

HIRT-PUB07001: Animation for the introduction of HIRT activities is now available : Hitachi Incident Response Team : Hitachi. (n.d.). Www.hitachi.com. Retrieved December 8, 2022, from https://www.hitachi.com/hirt/publications/hirt-pub07001/index.html