Information Security Policy

(Information Technology & Human Resources)

This Document was written and prepared by J & E Hall Limited. Its use is **CONFIDENTIAL** and must only be used as an internal document. Written authority from a company Director must be obtained prior to circulating this document to any third party

Prepared By:	Jamie Lovesey & Simon Young	**Copy No.:**	1
Title:	IT Manager/Technical Publications Author		
Reviewed by:	Jamie Lovesey & Andrew Bowden	**Authorised by:**	Andrew Bowden
Title:	IT Manager/Managing Director	**Title:**	Managing Director
Signed:	Jamie Lovesey	**Signed:**	
Date of Issue:	01/04/2020	**Review Date:**	2022
Reference No.:	Information Security Policy	**Version No.:**	09
Supersedes:	Issue 8		

Amendment No.	Section No.	Page No.	Paragraph No.	Date	Amended By
2	3	9	3	16/01/2019	S. Young
2	7.9	15	7.9.4	16/01/2019	S. Young
2	7.10	15	7.10.8 and 7.10.9	16/01/2019	S. Young
3	3	4	3	30/1/19	A Batley
3	7.10	10	7.10.8	30/1/19	A Batley
4	7.7	9	7.7.1	27/03/19	J.Lovesey
5	7.1	12	7.13.4 and 7.13.5	03/12/19	J.Lovesey
6	7.1	11	7.7.3 and 7.7.4 and 7.7.7	9/06/20	J.Lovesey
7	7.12	11	7.12.1	29/06/20	J.Lovesey
8	4 7 7 7 7 7 7 7 7 7 8 9 14	6 9 10 10 10 10, and 11 11 12 12 13 14 16 19	4.1.4 and 4.1.7 7.1, and 7.2 7.3.4 7.4.3 and 7.4.4 and 7.4.5 7.5.4 7.6.1 and 7.6.2 and 7.6.3 and 7.6.4 7.7.9 7.8.7 7.9.6 7.13.3 8.1.6 9.1.2 and 9.1.4 14	16/02/21	J.Lovesey
9	3	4	3	01/04/21	J.Lovesey

Contents

1. Introduction & Scope

This document sets out the Information Security Policy for J & E Hall Limited for the protection of information assets and related systems and processes to ensure confidentiality, integrity and availability of information in any format.

This Policy is applicable to all J & E Hall Limited Business units, subsidiaries & personnel (ADC, C&P, DAPS).

2. Objectives

The objectives of this policy are to:

- Ensure confidentiality of information assets, protecting them against unauthorised access or disclosure;
- Ensure integrity of data and information assets, protecting them from unauthorised or accidental modification or corruption;
- Ensure availability and accessibility of Information and related systems when required;
- Raise awareness of the importance of Information security and embed the principles in the day-to-day business culture of J & E Hall Limited;
- Support the J & E Hall Limited business objectives;
- Support the legal obligations of J & E Hall Limited for example under the Data Protection Act 2018, the Copyright Patents and Designs Act 1988 and the Computer Misuse Act 1990, and the General Data Protection Regulations (EU) 2016/679 etc.

3. Responsibilities

The following table defines responsibilities for Information Security at J & E Hall Limited.

MD (COO)	The MD has the ultimate responsibility for Information Security and Data Protection at **J&E Hall Limited**
Director of Finance	The Executive with operational responsibility for Information Security and Data Protection at **J&E Hall Limited**
Director of HR	Responsible for Personal data: • Liaising with the IT Manager on Information Security Matters; • Managing General Data Protection Regulations (GDPR) on a day-to-day basis; • Reporting on GDPR issues and related activities to J & E Hall Limited Executive Management; • Providing specialist advice, guidance and approvals related GDPR; • GDPR Data Breach Management; • GDPR awareness training; • Providing advice and reviewing third party supplier and service provider contracts and appropriate due diligence in relation GDPR. • Ensuring all Staff can access the Electronic Communications and Social Media Usage Policy and receive adequate information and training in respect of the GDPR regulations.

IT Manager (IT & IT security Manager)	Responsible for IT related Information Security including: • Liaising with the Director of HR on Information Security Policy (this document) and related matters; • Managing IT related Information Security on a day-to-day basis; • Reporting on the IT related Information Security issues and related activities to J & E Hall Limited Executive Management; • Providing specialist advice, guidance and approvals related to use of IT in relation to Information Security; • IT related Security Incident & Breach Management; • Information Security awareness training; • Providing advice and reviewing third party supplier and service provider contracts and appropriate IT related Information Security due diligence; • The integrity of all central computer systems, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of the IT Department; • Ensuring Security patches are applied promptly and changes are controlled are managed appropriately; • Monitor IT security, revise and adapt the Information Security Policy (this document) to maintain security conditions.
Business Unit Directors	Responsible for Information Security not related to Personal or IT related Information Security. Incidents and breeches must be reported to the Director of Finance.
Directors, Managers, Team Leaders	Responsible for: • Data Protection and Security of Information Assets; • Promoting good Information security practices; • Supporting the IT Manager & Director of HR in ensuring compliance with Information Security Policy (this document); • Ensuring critical third party suppliers and service providers are appropriately security vetted and an appropriate contract is in place; • Ensuring Data Protection Impact Assessments are completed where appropriate; • Managing Information security risks and solutions; • Notification to customers or suppliers without unnecessary delay where a data breach is likely to adversely affect our customers or suppliers.
System Administrators	Are in a position of trust within the organisation responsible for: • Ensuring they act appropriately and access accounts and systems only in a support situation, where authorised or appropriate; • Reporting any perceived weakness, breach or incident; • Monitoring systems and logs.
All staff	Are responsible for: • Complying with Information Security Policy (this document) and Procedures; • Read, understand and comply with the Electronic Communications Policy; • Protecting internal, confidential and personal data and ensuring it is handled appropriately and secure; • Reporting errors, suspected incidents or issues concerning IT security immediately to the IT Manager; • Reporting errors, suspected incidents, data breaches or issues concerning personal data and non IT security immediately to the IT Manager & Director of HR; • Staff with permissions for installing software on their own machine are responsible for ensuring it remains patched and supported by the supplier. If the supplier ceases to patch the software, it must be removed.

4. Information Asset Management & Classification

4.1. Information Asset Management

4.1.1. J & E Hall Limited will maintain a Personal Data and IT Equipment Asset inventory, owners of the assets will be defined in the asset register.

4.1.2. This will include but not be limited to IT equipment, which be uniquely identified and recorded. Records of all faults and suspected faults will be maintained against that asset.

4.1.3. All company assets must be returned to J & E Hall Limited on termination of contract or leaving the organisation by following the SLAM (starter, Leaver, and Movers) process which can be found on Cascade.

4.1.4. For security only IT personnel can access this inventory database. This is to protect the license keys from unauthorised use or fraudulent activity.

4.1.5. The IT Department uses a hardware and software inventory tool to intelligently discover installed software and devices across the network. This information will be used to audit and reconcile the Company inventory records to ensure the Company has a legitimate software licenses.

4.1.6. The IT Department reserve the right to monitor use of IT assets and where they determine misuse or negligence in use of IT equipment or Information, this will be reported to the users Line Manager and HR Department.

4.1.7. Any “cloud system (dropbox, Azure, salesforce etc)” usage must be requested via the IT Security Manager using a BIA (Business Impact Assessment form). The BIA request will specify its purpose and the type of data it will hold. The cloud service will then be checked for any security vulnerabilities, known threats, and will be risk accessed prior to approval. Any cloud systems data centre must reside in the UK or EU, failure to meet this requirement will be a non-conformity and be rejected due to data protection and copyright laws being different in other countries leaving our data ownership at risk (ie Facebook is American based and they own the data put on their platform). Once the BIA has been accessed the IT manager and MD will decide if to approve access.

4.2. Information Classification

4.2.1. The Company attaches great importance to the secure management of the data it holds and generates and to aid secure handling of data all Information at J & E Hall Limited will be classified into one of the following categories, these categories will govern and guide how that information will be handled to ensure adequate security.

4.2.2. J & E Hall Limited do not require that all information be marked with its classification.

4.2.3. GDPR/Data Protection - The Company is the controller and processor of Personal Data and therefore is required to comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

4.2.4. Please refer to the GDPR/Data Protection Policy for further information but be mindful of the following:

4.2.5. Personal Data will be classified as confidential and must be kept secure and must not be used, accessed or disclosed to any third party unlawfully.

4.2.6. Individuals have the right to see their ‘personal’ data and therefore care must be taken to record facts and not opinions as these would be disclosable under the individual’s subject access rights.

4.2.7. Data protection closely overlaps with information security and both must be considered where personal data is involved.

4.3. Asset Secure Disposal

4.3.1. All IT equipment must be disposed of via the IT Department. IT equipment must not be sold or donated without data sanitisation and management approval.

4.3.2. All items of IT equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed, data securely overwritten in line with 5220.22-M or more recent NIST 800-88 standards prior to re-use or hard discs destroyed prior to disposal or re-use.

4.3.3. All IT Hardware will be disposed of in line with the Waste Electrical and Electronic Equipment (WEEE) Regulations (as amended).

4.3.4. Disposable Media shall be returned to IT, to be destroyed or securely wiped prior to disposal.

4.3.5. Internal or confidential waste will be disposed of securely.

5. Human Resources Security

5.1. Employee Screening

J & E Hall Limited carry out screening of personnel prior and in the early stages of employment, the following checks are made:

- Identity checks;
- Right to work in the UK;
- Qualifications if required for the job role;
- References.

5.2. Job Descriptions and Contracts of Employment

All contracts of employment clearly define employee's responsibilities to comply with data protection and Information Security.

Where employees roles have specific responsibilities or accountability for the management of Information Security these will be defined also in their Job Description.

5.3. Information Security Awareness

All staff will receive Information Security, Data protection and Secure data handling training during an induction and during their employment.

This may take the form of face-to-face training, discussions, emails, posters, computer based training, manager and peer support and documentation.

6. Physical & Environmental Security

6.1. Building/Office Security

All visitors will sign in and out and be escorted at all times.

6.2. Secure Areas

- Computer/Server Room.

The computer/server room areas are secured by employing the following controls:

- Digital door locks;
- Access to premise/server/communication rooms will only be with the express permission of the IT Department and visitors and users must be accompanied by an appropriate person;
- Eating and drinking is not permitted in these rooms.

All computer/server rooms are fitted with climate control.

6.3. Workspace Security

6.3.1. Any computer equipment must be locked by the user when being left unattended; as an extra precaution computers will be configured to auto lock out after a period of 10 minutes inactivity.

6.3.2. Confidential papers must not be left on desks when being left unattended or overnight; they must be locked away.

6.3.3. Printed documents must be collected promptly from printers, consideration must be given to using secure pins when printing confidential information.

6.3.4. All persons working on or with J & E Hall Limited systems or information must be aware of their surroundings especially in public places (e.g. trains, coffee shops) and who could see their screens, papers or overhear conversations.

6.3.5. Personnel must ensure windows, doors and cupboards are closed and locked overnight.

6.3.6. When being transported or temporarily left in a vehicle they must be hidden from view in the boot and must not be left in a vehicle overnight. When unloading a vehicle remove and secure J & E Hall Limited equipment and papers first.

7. IT & Operational Security

7.1. Computing Environment & Equipment

The IT Department manages, maintains and operates a range of central computing servers, systems, core network switches, backup systems, and the overall network infrastructure interconnecting these systems.

The computing environment is defined as all central computing resources and network infrastructure managed and overseen by the IT Department and all computing devices that can physically connect to it, and have been authorised to connect to this environment.

This Information Security Policy (this document) covers all computing hardware and software, any business related data residing on these machines or accessible from these machines within the business network environment.

To ensure prevention of loss or damage or compromise of assets or interruption to the organisations operations equipment will be:

- IT operating procedures will be documented and available to appropriate personnel;
- Computing resources not owned by the business may be connected to the Company Guest Wi-Fi only for minimal personal use (during breaks) so long as appropriate for the workplace. Devices must be running up to date anti-malware software where possible;
- J & E Hall Limited provides computing equipment and facilities are principally for business use; refer to the Electronic Communications Policy;
- All IT equipment must be procured with the knowledge and agreement of the IT Department;
- Software must only be procured and configured with the knowledge and agreement of the IT Department;
- Processing and storing business data on non-Company devices is prohibited; refer Electronic Communications Policy.
- A standard laptop, server, and tablet image is to be used and is to be checked for vulnerabilities monthly using vulnerability scanning software. Any Critical, important, or service patches identified will be updated to the image. These scans will be recorded for reference. We will also follow NCSC (National Cyber Security Centre) for reference and guidance for most recent information.
- Any new system request will be requested via a business case document to highlight requirements, a business impact assessment document will be used to highlight security risks.

7.2. Change Control

All changes to IT infrastructure and software will be carefully controlled using a “IT change form”, considered for consequential risk, tested if applicable, planned and authorised before being applied.

7.3. Malware Protection

7.3.1. All computers will run approved anti-virus software at all times, which will be configured to:

- Scan on access;
- Update daily.

7.3.2. Any machine that is not able to support the latest anti-virus software and associated updates will be removed from the network.

7.3.3. Internet access will be protected web-borne malware and viruses using anti malware software. Refer 13. Audit and Compliance and the Electronic Communication Policy for further information.

7.3.4. Users are told not to click on suspicious email links or go into suspicious websites. We use malware EDR software that checks links and attachments against the software providers known central database which is updated with real time threat hunting. If the link is suspicious it is blocked so the user can't access the link, if it's an attachment the email checking provider validates the safety by sandboxing this in their safe environment, and if deemed safe it is released to the user, if a threat the attachment is blocked from access.

7.3.5. Our malware software blocks untoward activity on all devices and informs us via email.

7.4. Logging & Monitoring

7.4.1. The Company reserves the right to monitor, log, collect and analyse the content of all transmissions on networks maintained by the Company and individual Departments and at any time deemed necessary for performance, capacity and stability, fault diagnostic and for purposes of compliance with the Electronic Communications Policy.

7.4.2. The clocks of all core IT systems will be synchronised with a central recognised time source to ensure accurate log information.

7.4.3. All laptops / desktops record local event logs, if a security metric is triggered by our centrally managed security software or if a user tries to install software onto their device an event notification and the action the security software took is emailed direct to IT department email account.

7.4.4. All failed login attempts are logged, and an email is sent to IT email account if the account is suspended due to failed login attempts.

7.4.5. Network equipment is constantly monitored, and email event alerts are setup to inform the IT department.

7.5. Backups

Users local 'My Documents folders and desktop' are backed up to either the local NAS drive or an appropriate centrally managed file server. Backups are kept for 3 months.

The NAS drive is backed up daily to the Dartford based file server.

File servers are backed up daily to tape and are stored at another J & E Hall Limited site.

IFS and MS Exchange systems are hosted by a third party partner and are backed up daily to a SAN and secure offsite storage.

7.5.1. User devices that are not regularly on the network are recommended to be connected at least once a week and important documents saved to network storage; such users are provided with portable storage devices to back up to.

7.5.2. When an employee leaves the Company employment their Login is automatically disabled via the HR System and Active Directory, the IT Department will arrange to take a backup copy of the machine data, and then remove the data from the machine.

7.5.3. All email traffic is backed up on a daily basis.

7.5.4. IFS and fileserver backup data will undergo test restores bi-annually to ensure data is retrievable in the event of a disaster and meets the Recovery Time Objective (RTO). A test report will be produced and stored for monitoring the recovery time taken and ensure original recovery timeframe objective is still met. Our 3rd party support consultants will test the IFS database restore, internal IT staff will test random NAS and fileserver data restores.

7.6. Vulnerability & Patch Management

7.6.1. Any new software that has been procured is vulnerability scanned prior to deployment. If the software highlights non-conformity the software is not introduced into the environment and an alternative is researched.

7.6.2. As part of our continuous security monitoring, we run monthly vulnerability scans of our network, website and user devices. Any vulnerabilities highlighted are addressed and rectified.

7.6.3. Critical & Important Patches released for Operating system and 3rd party applications will be applied within 14 days of release to meet the Cyber Essentials PLUS requirement. Devices that are not connected to the network will not update, if they are unable to connect to a network this is the only exception allowed. However, they will update automatically when they reconnect to the network internally or externally as the patch software is cloud based reducing the risk of vulnerabilities being exploited.

7.6.4. Users have the rights to install applications themselves on their device but our patch management software will validate the software in a sandbox environment and check for vulnerabilities or errors in coding prior to instal. This is to ensure users are not introducing vulnerabilities onto their device.

7.6.5. End of Life Software (EOL) will be managed using our patch management tool, any EOL software will be uninstalled. EOL software is classified as supplier ceases support or issuing of patches.

7.6.6. Vulnerabilities will be monitored as part of an annual penetration test; identified vulnerabilities will be assessed on a risk basis and mitigations applied as deemed appropriate.

7.7. Encryption

7.7.1. The Company information system resources shall be appropriately protected to prevent unauthorised access by applying a level of encryption to internal or confidential information, which is proportionate to the business risk.

7.7.2. All encryption will be FIPS 140-2 compliant or equivalent with a minimum 128bit.

7.7.3. All Windows 10 laptops and desktops are to be encrypted using full disk encryption in accordance with NCSC data at rest guidelines.

7.7.4. Windows 7 laptops that are not required to interact with machinery based systems are to be encrypted or replaced by Windows 10 encrypted laptops.

7.7.5. Windows 7 laptops that interact with machinery based systems and are unable to be encrypted due to 3rd party software limitations are to be exempt from this policy. They must not access any government encrypted required contracts data.

7.7.6. All confidential and some internal information (if deemed necessary) transferred outside of the Company must be encrypted.

7.7.7. Removable media, including memory sticks must be encrypted if used for internal or confidential data. Where this is not feasible for business reasons an exception to policy will be made. The Business Unit manager or line manager reporting into the BU manager can approve in the form of an email being sent to the IT department. The IT Manager and Exec will then measure the risk and approve or deny.

7.7.8. Where BitLocker is deployed the encryption keys are managed by the IT Department.

7.7.9. E-mails or content containing confidential information is to be encrypted.

7.7.10. All individuals are responsible for ensuring that confidential information is encrypted before leaving the Company premises or network.

7.7.11. Where necessary, encryption keys are securely managed in a central location such that all information encrypted by the Company can be decrypted if required.

7.7.12. All Laptops and Desktops will have USB encryption enabled meaning prior to writing or moving data onto the USB it will request an access password and then encrypt the data. All new USB pens connected to a device will request a password prior to use. The machines exempt from this rule are windows 7 engineers laptop where they copy control data to SCADA machines, SCADA machines cant decrypt USB’s.

7.8. Network Security

7.8.1. Firewalls are deployed in every Company office between the network perimeter and the internet and between other offices where there is network traffic.

7.8.2. Firewalls are configured on an open on exception basis, ensuring ports are closed unless there is a valid business reason to open and configure that port.

7.8.3. Default firewall passwords is changed to meet complexity requirements before deployment, refer to 8. Access Control.

7.8.4. Network segregation will be considered where appropriate to limit risk.

7.8.5. Firewalls will only be accessible and configured by authorised persons.

7.8.6. Network communications security will be monitored to ensure security and protect against intrusion, availability or vulnerability risks.

7.8.7. All unused data points are disabled at the switch to prevent unauthorised access onto the network.

7.8.8. The network diagram is to be maintained and kept upto date at all times.

7.9. Email Security

7.9.1. J & E Hall Limited provided email must be used for all business related email, personal email accounts must not be used for work purposes.

7.9.2. All copy of all email traffic will be archived.

7.9.3. Email accounts are disabled when an employee leaves as part of their login decommissioning and retained.

7.9.4. Microsoft Exchange Sync to mobile devices is only permitted to Company owned devices unless expressly permitted by the Managing Director.

7.9.5. Confidential information must not be emailed without use of Encryption – see the Encryption Section in this document.

7.9.6. O365 uses secure channel to exchange emails with other email servers. Our emails will have arrived over an encrypted channel, O365 uses "Opportunist TLS" meaning Microsoft will encrypt the email, but fall back if the client mail server is to old.

Refer the Electronic Communication Policy for further information.

7.10. Data Storage & Transmission

7.10.1. Consumer cloud storage services are not suitable for confidential, or internal information and must not be used.

7.10.2. Centrally managed file storage must only be accessed by those who have permission, and only via secure, authenticated connections.

7.10.3. Internal and confidential paper information must be stored securely when not in use.

7.10.4. Access to electronic internal and confidential information will be controlled by use of network login permissions. Users must not attempt to access information they have not been authorised to access.

7.10.5. Confidential information must not be transmitted or transported without adequate encryption, refer to 7.7. Encryption.

7.10.6. Confidential information must not be shared, hosted or processed by a third party without due diligence and appropriate approvals.

7.10.7. Employees must avoid storing confidential information on portable equipment whenever possible.

7.10.8. Information related to project financials will be retained in the Corporate business system ‘IFS’.

7.10.9. All project information is stored on J & E Hall owned servers located on our own premises or our own servers located in a datacentre.

7.11. Internet Security

7.11.1. Internet filtering will be used to ensure appropriate content and use of the internet.

7.11.2. Guest Wi-Fi access to the internet will be offered via a separate guest Wi-Fi network only.

7.11.3. Guests must be made aware web browsing is monitored and recorded.

7.11.4. Staff may use the Guest Wi-Fi for minimal personal use during breaks, however their use must be appropriate for the workplace.

7.12. MS Office 365 Teams

7.12.1. Microsoft Teams is to only be used for video conferencing and team Messaging. No documents are to be transferred into MS Teams, only screen sharing is to be used when working collaboratively and sharing a document.

7.13. Remote Access to Systems

Remote access is defined as accessing systems from a physically separate network.

7.13.1. Remote access to Company information or systems must be via the secure VPN remote access solution provided using authorised logins, and authorised corporate devices only. No personal devices are to be used as security software can’t be guaranteed to managed and kept upto date.

7.13.2. All remote connections are logged.

7.13.3. If software allows 2 Factor Authentication, it must be used to gain access to systems remotely to confirm the authenticity of the user.

7.14. Mobile devices (Smart phones and tablets)

7.14.1. All smartphones, tablets or other smart devices used for work purposes shall be encrypted.

7.14.2. All smartphones and tablets intended for work use shall be capable of being encrypted.

7.14.3. Mobiles shall be no older than 4 years old due to firmware and security patches not updating beyond this period.

7.14.4. Use MDM software to ensure each device is built to the same specification, is locked down so only pre-approved applications can be installed from the app stores, and so it can be remotely wiped.

7.14.5. All smartphones are to be secure and hardened, after 4 failed login attempts a prompt must popup to inform you that you have 4 more attempts before the device resets itself to default settings.

8. Access Control

8.1. Logical Access Control

In order to protect J & E Hall Limited IT systems and information within them from unauthorised access, access to them will be individually controlled and permitted on a need to know basis.

The following Policy statements must be observed.

8.1.1. Any portable equipment (such as laptops, tablets, mobile phones, memory sticks, CDs, etc.) must use a log-on or power-on password.

8.1.2. All logins must be:

- Appropriately authorised and permissions approved;
- Unique to the individual and must not be disclosed or shared;
- Allocated permissions for job role basis and will be reviewed on role change within the organisation;

8.1.3. Default passwords will be removed or replaced with complex passwords immediately before deployment.

8.1.4. Unrequired applications, services will be removed from equipment or disabled before deployment.

8.1.5. Requests to change access permissions must be made in the first instance to the IT Department for verification of the requirement for change.

8.1.6. If a user requires access to a particular network folder, the user will need to request access via the folder owner, there is document register on the server that identifies who the folder owners are. The folder owner will then email IT Support approving what access is to be granted to the requesting user.IT will then email both owner and user when access has been applied. If the folder data is GDPR related only the MD and HR can approve access.

8.1.7. User accounts and permissions will be reviewed on a regular basis by the system and information owners with the IT Department. The review will be logged and the IT Department will sign off the review to give authority for users' continued access rights.

8.1.8. Consideration will be made to segregate sensitive duties to reduce risk of opportunities for unauthorised or unintentional modification or misuse of the Company assets.

8.1.9. Where possible requests to revoke access should be made in writing however it is acknowledged there may be emergency situations when a call may be sufficient, in which case, this will be logged.

8.1.10. Access for remote users will be subject to authorisation by the IT Department. No uncontrolled external access will be permitted to any network device or networked system.

8.1.11. Logins must not be disclosed to any other person or be shared, users must not permit anyone to login or use a computer logged in as them. An exception to this would only be if IT staff needed to provide support under a user's login.

8.1.12. Users will be allocated, by IT, a unique password on commencement of employment.

8.1.13. Passwords must be changed immediately if the user suspects that their account has been compromised.

8.1.14. Passwords will be complex and must contain the following criteria:

- Minimum 8 characters long;
- Minimum 2 letters;
- Minimum 6 digits.

8.1.15. Network Logins will lockout after 5 failed login attempts in a 30 minute period and remain locked for 60 minutes.

8.1.16. Passwords/PIN numbers or fingerprint must protect portable electronic devices such as Smartphones and Tablets. Pins will be a minimum of 5 characters in length.

8.1.17. Data will be managed in accordance to contract requirements, and will be held for the duration specified within the contract.

8.1.17 When an Employee leaves the Company the SLAM (Starter/Leaver and Mover) process will be triggered, their line manager, business unit manager or HR must notify the IT Department by either email or a Workflow Task generated from the HR Systems.

IT Department will:

- Disable the user login account and email account;
- Archive and retain indefinitely the users non personal data. Access to archived data is only with the express permission of the appropriate Director or the Director of HR;
- Recover any IT Equipment with the assistance of the Line Manager.

Line manager will:

- Ensure recovery and return of IT equipment to the IT Department;
- Recover any non-IT company equipment, keys and security pass/fobs.

8.2. System Administrators

8.2.1. System Administrators are authorised as part of their role set up to be an administrator by the Governance Group, who will also review such privileges regularly.

8.2.2. Administration tasks will only be carried out under an administrator login.

8.2.3. Administrator logins will be prevented from accessing the internet or using email.

8.2.4. Administrator Passwords must contain the following criteria:

- Minimum 8 characters long;
- Minimum 2 letters;
- Minimum 6 digits.

8.2.5. System administrators will operate in a position of trust and it is accepted that they may need to access or disclose information with appropriate authorisation:

- On all occasions System Administrators must seek individual authorisation from the appropriate person for the specific action that needs to be taken. Such activities may have legal implications for both the individual and the Company and therefore records must be kept to help protect all parties from any charge of improper actions;
- System Administrators must always be aware that their privileges grant them a position of considerable trust. Any breach of trust, by misusing privileges or failing to maintain high professional standards could be considered as gross misconduct.

9. Incident Management

All incidences of loss or theft of confidential information must be reported so that they may be investigated to the IT manager. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information either inside or outside the Company.

A security incident is any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised person;
- The integrity of the system or data being put at risk;
- The availability of the system or information being put at risk;
- Adverse impact, for example:
  - Negative impact on the reputation of the Company;
  - Threat to personal safety or privacy;
  - Legal obligation or penalty;
  - Financial loss or disruption of activities.

9.1.1. All actual or perceived incidents must be reported to the IT Manager, who will then inform HR and MD.

9.1.2. If an incident occurs the Incident Response Plan (IRP) document will be invoked and followed.

9.1.3. Security incidents in some case may also be a data breach and this must be considered.

9.1.4. In the case of a serious potential information breach the IT Manager or Director of HR will open an investigation into the incident. They will then follow the communication cascade located within the Incident Response Plan and report to any regulatory bodies, persons affected or other third parties, e.g. insurers, Daikin G.O.D. JEH Compliance manager.

9.1.5. The IT Department will retain a central register of all such incidents occurring within the Company. The HR Department will retain a register of any GDPR incidents occurring within the company.

The following examples of security incidents and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident the IT Manager & Director of HR should be informed who will then decide whether a report should be made.

9.2. Examples of a security incident

- Loss or theft of computer equipment or information due to crime of carelessness;
- Loss of portable media devices, e.g. – memory sticks etc.;
- Accessing any part of a database using someone else’s password;
- Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which computer equipment exists;
- Leaving confidential information or portable equipment unattended or a PC unlocked and unattended;
- Any breach of this Information Security Policy;
- Emailing confidential information to the wrong person or without encryption;
- Posting information to the wrong person;
- Finding confidential/personal information either in hard copy or on a portable media device outside company premises;

- Finding any records about employees or applicant in any location outside company premises;
- Unauthorised access to information or systems.

10. Supplier & Third Party Security

J & E Hall Limited require due diligence checks to be carried out on all critical suppliers and third parties, these will comprise of:

- Appropriate contacts and agreements;
- Information Security assessment by way of a questionnaire if required and a site visit if required;
- Finance and Purchasing checks;
- Review by the Purchasing Manager and HSQE Manager are to be undertaken in the first instance, and annually reviewed to ensure up to date thereafter
- GDPR checks by way of a questionnaire.

11. Risk Assessment & Management

All security controls are applied based on a risk assessment considering the impact and likelihood of the risk (Impact x Likelihood = Risk score) to ensure that information security risk is managed to ensure the confidentiality, integrity and availability of information and related systems.

The need for a Risk Treatment is based on the risk level and possible mitigations, possible risk treatment categories include:

- **Avoid** (mitigate to remove the risk);
- **Reduce** (mitigate to reduce the potential impact or likelihood of the risk);
- **Transfer** (insurance etc.);
- **Accept** (where there are no mitigations possible or the risk level is deemed acceptable.

11.1. Risks Management

11.1.1. Risk Treatments (Controls) are managed and applied when deemed necessary.

11.1.2. Risks will be recorded and scored on a risk register.

11.1.3. All risks will have a risk owner who will be responsible for ensuring the risk is managed.

12. Business Continuity & Disaster Recovery

J & E Hall Limited will consider business continuity risks when choosing IT infrastructure and planning, for the continuity of service provision in the event of a disaster situation.

A remote access VPN is used to provide access to corporate IT resources in the event of extreme weather or loss of building access.

The HR system is hosted externally to the corporate network to ensure continuity of staff management.

Some systems and backups are hosted externally to ensure continuity in the event of a network outage or disaster.

Care is taken to maintain information security in a disaster or business continuity situation.

13. Audit and Compliance

13.1.1. Compliance with this policy is mandatory and non-compliance may result in disciplinary; or legal action if deemed appropriate although this is not expected.

13.1.2. However If you make a mistake or discover a problem or incident please ensure you notify the appropriate persons (refer to: 3. Responsibilities) so that the risk and impact can be minimised; your prompt action will be considered in any action deemed necessary. It is important to remember that prompt and appropriate immediate actions can significantly reduce the impact of any incident or breach.

13.1.3. J & E Hall Limited carry our periodic reviews of security controls to ensure compliance and adequate security.

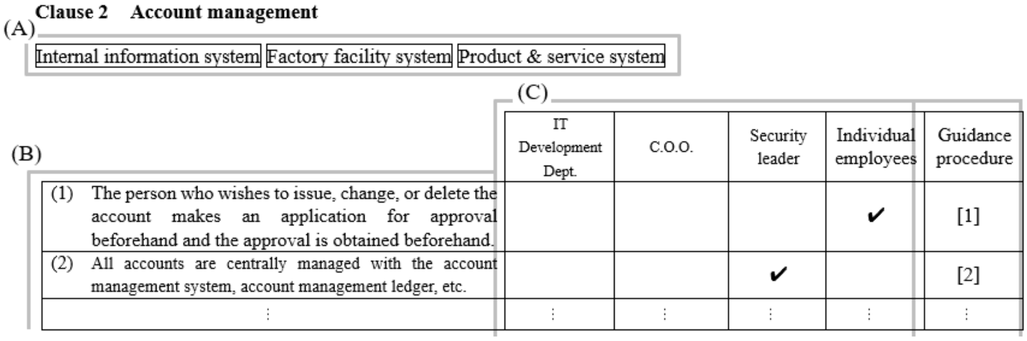
13.1.4. External reviews of network security are carried out on an annual basis.

13.1.5. The Company reserves the right to monitor, log, collect and analyse the content of all transmissions on networks maintained by both the Company at any time deemed necessary for performance, fault diagnostic and compliance purposes (Electronic Communications Policy). Logs will be available only to authorised systems personnel.

13.1.6. As part of the induction process at commencement of their employment, Employees are directed to the Electronic Communications and Social Media Usage Policy. Revisions to the Policy are advised through company communications.

13.1.7. Employees using corporate IT systems for anything personal must be aware complete privacy cannot be assumed but that it will be respected; there may be circumstances where logs or monitoring could capture personal information. This is therefore at the risk of the individual.

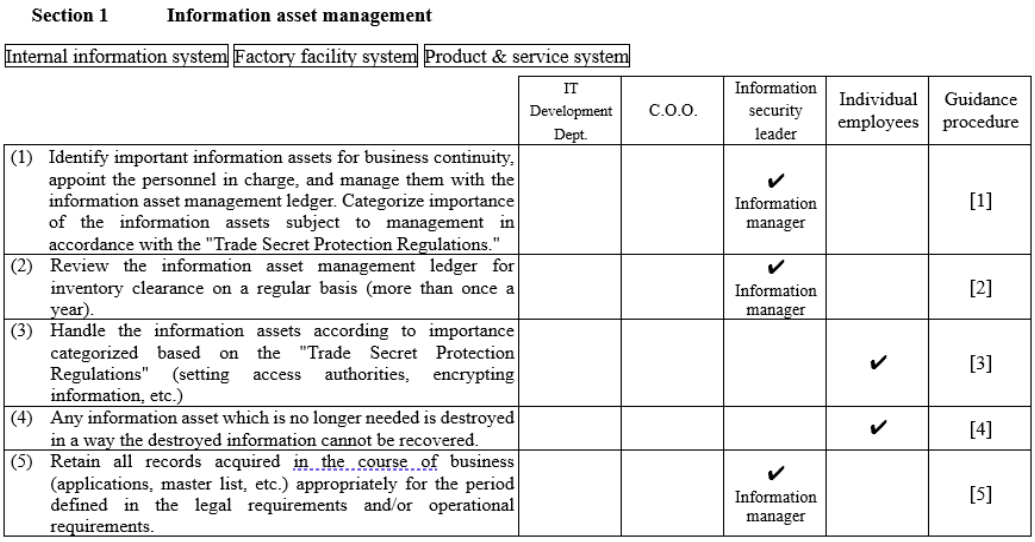
14. Daikin Security Management Accountability Matrix Reference



Clause 2 Account management

Internal information system | Factory facility system | Product & service system

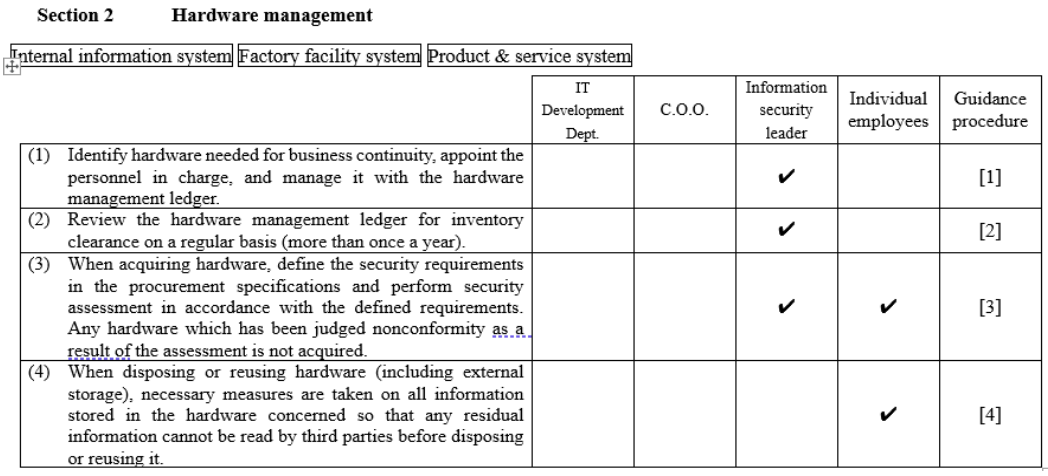
	IT Development Dept.	C.O.O.	Security leader	Individual employees	Guidance procedure	JEH ref
(1) The person who wishes to issue, change, or delete the account makes an application for approval beforehand and the approval is obtained beforehand.				✔	[1]	8.1
(2) All accounts are centrally managed with the account management system, account management ledger, etc.			✔		[2]	8.1
⋮	⋮	⋮	⋮	⋮	⋮	



Section 1 Information asset management

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Identify important information assets for business continuity, appoint the personnel in charge, and manage them with the information asset management ledger. Categorize importance of the information assets subject to management in accordance with the "Trade Secret Protection Regulations."			✔ Information manager		[1]	8.1, 8.1.6
(2) Review the information asset management ledger for inventory clearance on a regular basis (more than once a year).			✔ Information manager		[2]	8.1.6 8.1.7
(3) Handle the information assets according to importance categorized based on the "Trade Secret Protection Regulations" (setting access authorities, encrypting information, etc.)				✔	[3]	8.17
(4) Any information asset which is no longer needed is destroyed in a way the destroyed information cannot be recovered.				✔	[4]	8.1.18
(5) Retain all records acquired in the course of business (applications, master list, etc.) appropriately for the period defined in the legal requirements and/or operational requirements.			✔ Information manager		[5]	8.1.18



Section 2 Hardware management

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Identify hardware needed for business continuity, appoint the personnel in charge, and manage it with the hardware management ledger.			✔		[1]	4.1.5
(2) Review the hardware management ledger for inventory clearance on a regular basis (more than once a year).			✔		[2]	4.1.1
(3) When acquiring hardware, define the security requirements in the procurement specifications and perform security assessment in accordance with the defined requirements. Any hardware which has been judged nonconformity as a result of the assessment is not acquired.			✔	✔	[3]	7.1
(4) When disposing or reusing hardware (including external storage), necessary measures are taken on all information stored in the hardware concerned so that any residual information cannot be read by third parties before disposing or reusing it.				✔	[4]	4.3

Section 3 Software management

Internal information system Factory facility system Product & service system

	IT Development Dept.	C.O.O. or Security responsible personnel in the company	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Identify introduced software, appoint the personnel in charge, and manage it with the software management ledger.			✔		[1]	4.1.5
(2) Review the software management ledger for inventory clearance on a regular basis (more than once a year).			✔		[2]	7.6.5
(3) Manage the media for the licensed software with locking to prevent illegal copy.			✔		[3]	4.1.4
(4) Any program and/or data must not be duplicated unless it is required in the course of business. The duplicated data must not be taken outside the company unless it is required in the course of business.				✔	[4]	
(5) When using new software, perform security assessment. Any software which has been judged nonconformity as a result of the assessment is not introduced.			✔		[5]	7.6.1
(6) When using new cloud service, define the purpose and content and obtain approval by Information security leader, etc.			✔		[6]	4.1.7
(7) For the system connected to the Internet, the system provider should be specified, the person who wishes to open, change or abolish it must apply for approval, and the approval should be obtained beforehand. The operating conditions of the system connected to the Internet should be reviewed for inventory clearance on a regular basis (more than once a year).		✔	✔		[7]	7.2

Chapter 4 Management of employees and subcontractors

Section 1 Management of employees

Internal information system Factory facility system Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) The employment agreement with the employee specifies individual responsibility for information security, and the non-disclosure or similar agreement is concluded as needed.			✔		[1]	5.3
(2) Define the responsibility and duty for security which remains effective even after termination of the employment or any change to the agreement, and communicate it to employees and ensure their observance.			✔		[2]	5.2
(3) When the term of employment or the contract with the employee terminates, instruct the employee to return all information assets and other lent items and delete all of the information on the employee and his/her access right.			✔		[3]	4.1 4.3

Section 2 Management of subcontractors

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) When outsourcing development and/or operation work to external parties, define the criteria for selecting subcontractors including confirmation of the security management status and determine the subcontractor(s) in accordance with the criteria.			✔		[1]	10
(2) Information exchange is managed after the methods of transferring, receiving, returning and disposing information are determined beforehand.			✔		[2]	4.1.7
(3) Make sure to transfer and receive software, electric data, etc. with subcontractors, etc., in accordance with the predetermined procedure as defined in the previously agreed contract.			✔		[3]	10
(4) Manage information on the subcontractor companies (the names of the security manager and the security staff, their contact information, etc.) by listing them up, and confirm whether or not the information is kept up-to-date on a regular basis (more than once a year).			✔		[4]	10
(5) Confirm the security management status of the subcontractors on a regular basis (more than once a year). If any problem is detected, request the subcontractor to solve it and confirm what was improved.			✔		[5]	10
(6) At the same time when the subcontractor's work is finished, confirm all of the provided information is disposed and returned.			✔		[6]	10
(7) The outsourcing agreement specifies individual responsibility for information security, and the non-disclosure or similar agreement is concluded as needed.			✔		[7]	10

Section 3 Education and training

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O. or Security responsible personnel in the company	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Establish the security training plan to make information security knowledge and skills entrenched and maintained.	✔	✔	✔		[1]	5.3
(2) Provide information security training when employees join the company and on a regular basis (more than once a year) and confirm the training has been provided to all employees.			✔		[2]	5.3
(3) Provide training as part of the cyber attack protection activities to employees on a regular basis (more than once a year).	✔	✔	✔		[3]	5.3
(4) Manage the updates and timing for updating for information security education and update the content of the education as needed.	✔	✔	✔		[4]	5.3

Section 4 Communication

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Communicate this regulation to the target employees and subcontractors and ensure thorough implementation			✔		[1]	5.3, 10

1. **Specific procedures to be observed by the departments, etc.**

[1] When the employees join the company, the outsourcing contract is concluded, or at the time of revision of the regulations, communicate and disseminate the regulations and request for observance of the regulations.

Chapter 5 Facility, equipment and system security

Section 1 Facility and equipment security

Clause 1 Zone design

Internal information system Factory facility system Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) To specify the area that needs security, classify the facilities the department, etc. manages into the following 2 levels, and establish physical boundaries for the area boundaries. Level 1: the area where only the person in need, from among the employees, can enter. Level 2: the area where the employees and visitors can enter.			✔		[1]	6
(2) Establish individual access barriers in the Level 1 area to control entrance and exit so that only authorized personnel can enter and exit the area.			✔		[2]	6

Clause 2 Entrance/exist management

Internal information system Factory facility system Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) When access to the Level 1 area is needed, the authority to access the area is applied and the approval is obtained before the entrance.				✔	[1]	6.1
(2) Every entrance to /exist from the Level 1 area is recorded and managed.			✔		[2]	6.1, 6.2
(3) The authority for entrance is deleted immediately after it becomes unnecessary due to personnel transfer or retirement. At the same time, any lent ID card and other items are immediately returned.			✔		[2]	4.1.3, 8.1.17
(4) The authorities for entrance are reviewed on a regular basis (more than once a year). Any ID card and other items which are no longer used for a business reason are immediately returned.			✔		[4]	4.1.3, 8.1.17
(5) The process to easily distinguish between onsite personnel and visitors is developed.			✔		[5]	6

Clause 3 Bringing-out and carrying-in of devices

Internal information system Factory facility system Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) The person who wishes to bring out a device from the Level 1 area and carry a device in the area applies for approval beforehand and obtains the approval before bringing-out and carrying-in of the device.				✔	[1]	6.2
(2) When an external storage needs to be used, the person who wishes to use it applies for approval on use of the company-designated external storage with encryption function beforehand and obtains the approval before using it, and returns it within the usage period.				✔	[2]	6.2, 6.3.1
(3) Usage status of the company-designated external storage with encryption function is managed with the management ledger and reviewed on a regular basis (quarterly).			✔		[3]	6.2
(4) The device installed in the Level 1 area and the device installed in the factory for which anti-malware software is not installed are provided with the measure to prevent writing to the external storage.			✔		[4]	6.2
(5) Carrying-in of private PCs to the company and use of private external storages for business use are prohibited.				✔	[5]	6.2
(6) Bringing-out of PCs and external storages to outside the company is performed in accordance with the "Procedure for bringing out PCs and external storages" to prevent a theft, loss, etc. and if a loss is detected, it is immediately reported to the information security leader.				✔	[6]	6.2, 7.8.7

Clause 4 Protection of facilities and equipment

Internal information system | Factory facility system | Product & service system

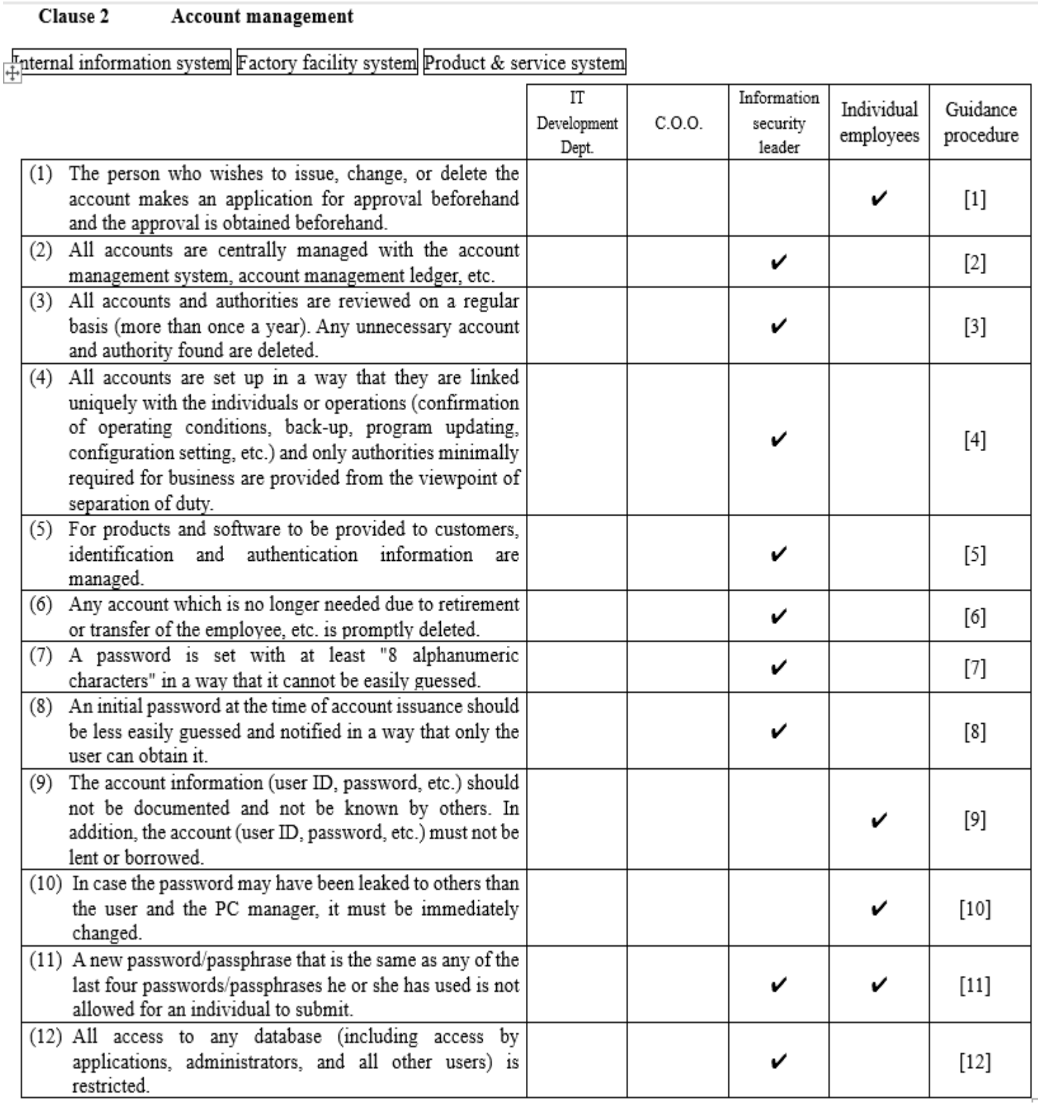
	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) The Level 1 area is provided with fire preventions (fireproofing, earthquake-proofing, and waterproofing), key locking, air conditioning, power supply system, etc.			✔		[1]	6.2
(2) PCs and external storages are stored with key locking to prevent theft.				✔	[2]	6.2, 6.3.1
(3) The devices and systems are mounted on server racks, etc. For any of them that cannot be mounted on server racks, some measures are taken to prevent theft with wire locking and fix the devices concerned.			✔		[3]	6.2
(4) The responsible person is allocated for management of the server racks and the server racks are managed with key locking.			✔		[4]	6.2
(5) Application for unlocking the server rack is made and the approval for unlocking is made beforehand and the status of lending and using the keys is managed with the management ledger.			✔		[5]	6.2
(6) Physical and/or logical controls is implemented to restrict access to publicly accessible network jacks.			✔		[6]	6.2

Section 2 System security

Clause 1 Configuration management

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Default configurations secured for each device and system are established and applied.			✔		[1]	7.1, 8.1.3
(2) For important work on the devices and systems, application is made for approval and the approval is obtained before the work is started.				✔	[2]	7.2
(3) For approval on changes to the device and system settings, the results of testing in the development environment, the results of reviewing the procedure, and others are confirmed.			✔		[3]	7.2, 7.6
(4) The versions of the configuration files, programs, etc. for the devices and systems are managed.			✔		[4]	7.6
(5) Only one primary function per server is implemented to prevent functions that require different security levels from co-existing on the same server.			✔		[5]	---
(6) Vendor-supplied defaults are always changed, and unnecessary defaults are removed or disabled before installing a system on the network.			✔		[6]	8.1.3, 8.1.4



Clause 2 Account management

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) The person who wishes to issue, change, or delete the account makes an application for approval beforehand and the approval is obtained beforehand.				✔	[1]	8
(2) All accounts are centrally managed with the account management system, account management ledger, etc.			✔		[2]	8
(3) All accounts and authorities are reviewed on a regular basis (more than once a year). Any unnecessary account and authority found are deleted.			✔		[3]	8, 8.1.17 8.1.7
(4) All accounts are set up in a way that they are linked uniquely with the individuals or operations (confirmation of operating conditions, back-up, program updating, configuration setting, etc.) and only authorities minimally required for business are provided from the viewpoint of separation of duty.			✔		[4]	8.2
(5) For products and software to be provided to customers, identification and authentication information are managed.			✔		[5]	10, 8.1.17
(6) Any account which is no longer needed due to retirement or transfer of the employee, etc. is promptly deleted.			✔		[6]	8.1.17
(7) A password is set with at least "8 alphanumeric characters" in a way that it cannot be easily guessed.			✔		[7]	8.2.4
(8) An initial password at the time of account issuance should be less easily guessed and notified in a way that only the user can obtain it.			✔		[8]	8.1.12
(9) The account information (user ID, password, etc.) should not be documented and not be known by others. In addition, the account (user ID, password, etc.) must not be lent or borrowed.				✔	[9]	8.1.11
(10) In case the password may have been leaked to others than the user and the PC manager, it must be immediately changed.				✔	[10]	8.1.13
(11) A new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used is not allowed for an individual to submit.			✔	✔	[11]	8.1.12
(12) All access to any database (including access by applications, administrators, and all other users) is restricted.			✔		[12]	8.2

Clause 3 Access control

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O. or Security responsible personnel in the company	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) For connection to external network (Internet, network in other bases, etc.), the purpose and descriptions are specified and C.O.O(or Security responsible personnel in the company), etc.'s approval is obtained.		✔	✔		[1]	7.13
(2) For connection to the Internet, firewalls are installed to shut off direct access from the Internet to internal servers.			✔		[2]	7.8.1, 7.8.2
(3) Communication requirements to be permitted for firewalls (IP address, port, protocol, etc.) are sorted out. Firewall settings are checked with communication requirements for consistency and proper setting on a regular basis (more than once a year).			✔		[3]	7.8.5
(4) IP addresses, services and ports of the connections from/to the devices and systems are minimally required.			✔		[4]	--
(5) Connection among the bases is made with the closed network and not via the Internet in principle. When unclosed communication service is used, closeness is secured.			✔		[5]	7.8.4
(6) When the system for remotely connecting the devices and systems is introduced, appropriate authentication method is adopted to prevent illegal access.			✔		[6]	7.13.3
(7) The person who wishes to newly use the Internet makes an application and obtains the approval from the information security leader before using it.				✔	[7]	7.2
(8) The information services, the users, and the information systems are grouped depending on usage applications.			✔		[8]	--
(9) Records for the employees' Internet access are checked for inappropriate usage. If any inappropriate usage is detected, cancelation of the usage permission, etc. is implemented.			✔		[9]	7.4
(10) Connection of private PCs and PCs owned by others than the employees (external consultants, external system maintenance personnel, etc.) to the internal network is prohibited.			✔		[10]	7.13.1
(11) When leaving the PC and desk, the personnel sets screen locking and keeps the desks clean to prevent data on the screen from being stolen and illegally operated by others.				✔	[11]	6.3.1
(12) When the server is to be open to the public, it is installed on the DMZ protected with firewalls.			✔		[12]	7.8.4
(13) Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks is made and kept updated.			✔		[13]	7.8.8
(14) All individual non-console administrative access and all remote access are secured using multi-factor authentication.			✔		[14]	7.13.3

◢ Clause 4 Malware countermeasures

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Anti-malware software is installed in the servers and PCs and pattern files are always kept up-to-date.			✔		[1]	7.3.1
(2) The system is provided so that the alert level is raised when malware is detected.			✔		[2]	7.3.5
(3) Any external storage to be connected to the servers and PCs is surely scanned with anti-malware software.				✔	[3]	7.3.4
(4) Free software and other similar programs on the Internet must not be carelessly used.				✔	[4]	7.3.4
(5) Any suspicious e-mail from an unknown source must not be opened and destroyed.				✔	[5]	7.3.4
(6) For any Internet connection point and access point outside the company where files which can be infected with malware are sent and received, anti-malware measures are provided on the possible infection route.			✔		[6]	7.3.4

Clause 5 Vulnerability management

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Residual vulnerable settings are checked for the devices and systems connected to the Internet at the time of system release and drastic change, e.g. vulnerability test, vulnerability scanning, penetration test, etc.			✔			7.6
(2) When application of urgent security patches is made from the responsible party, application of the target patches is examined immediately.	✔		✔		[2]	7.6.3
(3) Information on vulnerability in the devices and systems, released security patches, currently-prevalent cyber attacks is collected.	✔		✔		[3]	7.6.6

Clause 6 Data protection

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Data that falls into trade secret information is provided with proper access restriction in accordance with the Trade Secret Protection Regulations.				✔	[1]	4.2.2, 4.2.5 8.1.2, 8.1.8
(2) Handling of business data on private PCs is prohibited.				✔	[2]	7.13.1
(3) PCs and external storages to be brought outside the company are provided with some measures (encryption, etc.) to prevent information leakage in response to a theft, loss, etc.			✔		[3]	7.7.3, 7.7.7
(4) When the data is transmitted externally, access to the data concerned is controlled.				✔	[4]	7.96
(5) When the information is transmitted/received via the Internet, the communication is encrypted.			✔		[5]	4.2.3, 4.2.4
(6) Personal information and my numbers (national identification numbers) are handled with proper protection in accordance with "Personal information protection regulations and my number regulations."			✔		[6]	4.2.3, 4.2.4
(7) Files and databases that contain confidential information such as accounts and passwords to access the devices and systems are provided with access restriction and encryption in principle.			✔		[7]	4.1.4
(8) Encryption keys and encryption key information used for digital signature are properly managed.			✔		[9]	7.7.8, 7.7.11

Clause 7 Log management

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) The devices and systems are provided with time synchronization with the NTP servers.			✔		[1]	7.4.2
(2) Logs of important devices and systems are obtained. Log items to be obtained (time and date, category, event, source/destination IP addresses, etc.), log storage places, etc. are defined.			✔		[2]	7.4
(3) For access to the data which falls into trade secret information, the manager obtains the access log and checks the log for any suspicious access on a regular basis.			✔		[3]	7.4
(4) Logs of records of access, log-in, operation, etc. of accounts are printed out and stored. When privileged account is used, the log is checked on a regular basis.			✔		[4]	7.4.4
(5) Presence of logs is checked on a regular basis for appropriate printout of the logs to be obtained.			✔		[5]	7.4
(6) Important devices and systems (including network) are monitored for failure all the time.			✔		[6]	7.4.3
(7) Attempts (many attempts to log-in) of illegal access to the devices and systems connected to external network are monitored.			✔		[7]	7.4.4, 8.1.2

Clause 8 Back-up

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) The back-up policy for data and programs of the devices and systems (target items, frequency, storage place, access authority, etc.) are defined and regular back-up is performed.			✔		[1]	7.5
(2) The backed-up data and programs are stored on other servers or electronic recording media and appropriate access authorities are allocated and managed.			✔		[2]	7.5
(3) The procedure for recovering the backed-up data and programs is established and the recovery test is implemented.			✔		[3]	7.5.4

◢ Clause 9 Design and development

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Security check points are established in the system life cycle and any security issue is checked at each check point.			✔		[1]	7.1
(2) Security requirements are established at the time of requirement definition and design of the product and system requirements. Or, the design criteria is established at the time of requirement definition and design and observed.			✔		[2]	7.1
(3) The development environment and test environment are prepared besides the production environment, and sufficient amount of testing is performed before transition to the production environment. Necessary access controls are provided for the period between the test environment and production environment.			✔		[3]	7.1
(4) When rental servers and/or cloud services are used during the development work, the security requirements to be considered when cloud services are used are defined and communicated to the related parties.			✔		[4]	7.1.7, 7.10.1

Chapter 6 Risk and incident management

◢ Clause 1 Risk assessment and auditing

Internal information system | Factory facility system | Product & service system

	G.O.D	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Specific procedures for observing the security operational management regulations are defined in the procedures, etc. The established procedures, etc. are thoroughly communicated to the departments, etc.			✔		[1]	Managed by IT Risk Policy
(2) The status of observing the security operational management regulations is confirmed on a regular basis (more than once a year) and the "security measures implementation status report" is created. The created security measures implementation status report is submitted to C.O.O. The subsidiary submits its security measures implementation status report to the responsible department, and the responsible department reports the current situation including the subsidiary's situation to C.O.O.	✔	✔	✔		[2]	
(3) For those of the requirements in the security operational management regulations which are not observed, corrective measures are examined and the "security improvement plan" is created. The created "security improvement plan" is approved by department manager/president of the subsidiary and submitted to C.O.O.		✔	✔		[2]	
(4) For those that are subject to auditing by Daikin industries information security committee, required documents are promptly submitted.		✔	✔		[3]	

Clause 2 Incident response and report

Internal information system | Factory facility system | Product & service system

	G.O.D. IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) Creates the incident response criteria the department, etc. should implement as standard in case any information security risk is evident.	✔ (IT Development Dept.)				[1]	9
(2) Creates the response procedure for the department, etc. based on the incident response criteria and thoroughly communicates it to the department, etc.		✔	✔		[2]	9.1.2
(3) When an incident is found, it is notified to the related parties in accordance with the response procedure established in the department, etc.		✔	✔		[3]	9
(4) Properly collects information on the incident that has occurred and promptly reports it to C.O.O., etc. and action is taken in accordance with the instructions given by the responsible personnel. In addition, it is reported to IT Development Dept. and G.O.D. in accordance with the incident response criteria.				✔	[3]	9.1.1, 9.1.4
(5) If the incident reported from the department, etc. is judged as a major security incident and additional measures are required for the incident, instructions to take action are given to the information security leader.			✔	✔	[3]	9
(6) As to the incident that has occurred, prompt investigation to find the root cause is implemented and the action to prevent reoccurrence is reported to G.O.D., and implemented under the approval by G.O.D, etc. after confirmed by C.O.O.	✔ (G.O.D.)	✔			[3]	9.1.4

Clause 3 Business continuity plan/disaster recovery

Internal information system | Factory facility system | Product & service system

	IT Development Dept.	C.O.O.	Information security leader	Individual employees	Guidance procedure	JEH ref
(1) The department, etc. strives to achieve prompt recovery of the information security in accordance with the Business Continuity Plan which is separately defined.			✔		[1][2][3]	12
(2) An uninterruptible power supply (UPS) should be provided.			✔		[4]	12

15. Related Documents

The following documents relate to this Policy:

- Electronic Communications and Social Media Usage Policy;
- GDPR Policy and procedures;
- Waste Electrical and Electronic Equipment (WEEE) Regulations (as amended);
- Computer Misuse Act (as amended);
- General Data Protection Regulations (EU) 2016/679;
- Data Protection Act (as amended);
- Copyright Patents and Designs Act (as amended);
- Business Continuity Plan:
- Cyber Security Plan.
- BIA Business Impact Assessment form
- IRP Incident Response Plan policy
- IT Security Risk Management Policy

End

This page intentionally blank.