Information Classification Policy

Version: 0.2
Date:20.03.2023
Created by: GDPR Local
Stored at: Safe Storage

1. Introduction

The Conservatory Insulation Company is committed to GDPR and data security. We recognise that information is a vital asset to any organisation and take our responsibilities under the GDPR seriously. Virtually all of our activities create information assets in one form or another. This Information Classification Policy is concerned with managing the information assets of our organisation.

The goal of this Information Classification Policy is to ensure:

- Availability, integrity, and confidentiality are provided at the necessary levels for all identified data assets
- Return on investment by implementing controls where they are needed the most
- Map data protection levels with organisational needs and the need to protect personal data
- Mitigate threats of unauthorised access and disclosure
- Comply with legal and regulatory requirements
- Protect the interests of our customers, suppliers, employees, and all other data subjects

2. Principles

Information asset classification ensures that individuals who have a legitimate right to access a piece of information can do so, whilst also ensuring that assets are protected from those who have no right to access them. This policy ensures that correct classification and handling methods are applied and managed accordingly. This policy is based on the requirement that:

- All information assets must be handled and managed in accordance with their classification
- Information assets should be made available to all who have a legitimate need to access them
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events;

- All individuals who have access to information assets, have a responsibility to handle them in accordance with their classification
- We respect the rights of all data subjects as defined by the GDPR

3. Objectives Of This Policy

- To define the responsibilities of individuals for safeguarding information assets
- To provide a rigorous and consistent classification system which ensures that information assets are appropriately protected and managed in accordance with the legal requirements
- To minimise the damage to the organisation, its customers, and partners as a result of sensitive information assets being intercepted or exposed
- To ensure that information assets which are lost, stolen, damaged or intercepted are sufficiently protected and unreadable so that unwarranted action cannot be taken against the organisation
- Protect the interests of our organisation, employees, customers, suppliers, and other data subjects

4. Action Implementation

Where these do not already exist, these procedures will be put in place to ensure that this policy is effective. These procedures include:

- Information users being appropriately identified and having access to information for which they have a legitimate need
- Information assets being appropriately managed and controlled in line with the requirements of this policy
- Information assets being identified and sufficiently protected in line with the correct categorisation and handling methods
- Ensuring that adequate control mechanisms are in place for protecting information assets
- Ensuring that information access control mechanisms are in place and that these mechanisms are reviewed regularly
- Ensuring that asset owners define the required physical security of computer rooms, networks, personal computers and procedures for computer maintenance
- Ensuring the safe disposal of all information assets and equipment
- Ensure we are able to respond to requests as required by the GDPR

5. The GDPR

The GDPR requires the organisation to ensure appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of or damage to, personal data.

6. Asset Classification And Handling

Information assets that are sensitive or have value must be protected at all times. Consideration must be given to day-to-day activities and protection outside normal working hours. All information should be classified into one of the following categories by those who own or are responsible for the information.

- Public
- Open
- Confidential
- Strictly Confidential
- Secret

Much of the information will fall into the Public or Open categories, but for good reason, such as personal privacy or protection of Volume Network LTD interests, some information assets may be categorised as “Confidential” or “Strictly Confidential”.

In exceptional circumstances information may be classified as “Secret”. In the event of uncertainty or disagreement as to the classification of the information asset, it is advised that the default category and handling methods should be Confidential or Strictly Confidential.

Where no classification is assigned, information should be treated as “Confidential”.

7. Asset Classification Categories, Type And Handling Methods

Public

May be viewed by anyone, anywhere in the world.

Public information assets may include but are not limited to:

- Principal contacts e.g. name/email address/telephone numbers for public-facing roles will be made freely available
- Announcements from authorities
- Publications
- Press releases

Please note some contacts are associated with specific job roles and responsibilities only and should not be released to the general public without consent.

Open

Access is available to all authorised company personnel [employees, contractors, and authorised third-parties].

Open information assets may include, but are not limited to:

- Contacts e.g. name/email address/telephone number
- “Approved” communications e.g. news/updates to ensure their relevance to day to day activities
- Policies/procedures/processes

Secure handling may include, but is not limited to:

Information should be formatted to enable basic security e.g. word documents converted into PDF to discourage tampering and disrepute. These include documents such as but not limited to:

- Procedures
- Policies
- Guidelines
- Customer information
- Financial information

Confidential

Access is limited to specified people with appropriate authorisation or on a need-to-know basis.

Confidential information assets may include but are not limited to:

- Personal details or identifiable information (name/address/telephone number/email address/date of birth/National Insurance number/ethnic or racial origin/religious beliefs, physical or mental health/sexual life/political opinions/trade union membership/the committing or alleged committing of criminal offences).
- Financial information
- Information relating to the private well-being of a person
- Wage slips/pay/pension/other employment documentation
- Death certificates
- PDR documents
- Employee contract data
- Non-Disclosure Agreements
- Documents in "draft“ format

Secure handling should be considered and may include, but is not limited to:

Paper Documents (In transit/rest)

- Secure locked storage (files/folders/cabinets)
- Approved third-party courier
- Use sealed envelopes instead of the usual transit envelopes
- Secure disposal

Electronic Information assets (In transit/rest)

- Encryption
- Password protection
- SFTP (Secure file transfer protocol)
- Secure file stores
- Secure disposal
- Reduced access rights/level of privileges

Strictly Confidential

Access is controlled and restricted to a small number of named

individuals/authorities

Strictly Confidential information assets may include but are not limited to:

- Bank details (sort code/account number)
- Credit Card Details (PAN/CVV2/Expiry Date/PIN)
- Financial data
- Medical records
- Servers
- Server rooms
- Usernames and passwords
- Test data
- Investigation
- Disciplinary proceedings
- Submitted patents/IPR
- Third party contract/supplier information
- Infrastructure or network information (including hardware and software)

Secure handling should be considered and may include, but is not limited to:

Paper Documents (In transit/rest)

- Secure locked storage (files/folders/cabinets)
- Approved third party courier
- Use sealed envelopes instead of the usual transit envelopes

Electronic Information assets (In transit/rest)

- Encryption
- SFTP (secure file transfer protocol)
- Secure file stores
- Asset tags
- Secure disposal
- Access rights/Level of privileges

Secret

Access is subject to or obtained under the Official Secrets Act.

Special circumstances may require differing controls above/or below) local circumstances. Each requirement will be reviewed on a case-by-case basis in line with HMG controls. HMG advice and guidance is subject to regular change.

8. Classification Guidelines (Paper/Electronic Copy)

Classification markings are considered mandatory for “Secret” documents only and, where used, must be clearly visible on all information assets containing a category of classification information. The appropriate markings are to appear clearly either at the top, in the centre or at the bottom of each page.

9. Re-classification Of Information Assets

Some information assets may be reclassified from one category to another based on the content and intent of the asset. There must be sound reasoning for the reclassification. If there is any doubt over the classification of an asset, contact the Information Security Officer.

10. Sensitive Information Assets

Responsibility for definition and the appropriate protection of an information asset remains with the originator or owner. A higher level of protection must be provided for sensitive information assets which includes ‘personal data’ and ‘personal identifiable information’, which is defined as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership or the committing or alleged committing of criminal offences.

Identifying sensitive information is a matter for assessment in each individual case. Broadly speaking, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

- Financial loss e.g., the withdrawal of a grant or donation, a fine by the ICO or a legal claim for breach of confidence
- Reputational damage e.g., adverse publicity, demonstrations, complaints about breaches of privacy; and/or
- An adverse effect on the safety or well-being of staff of the organisation or those associated with it e.g., increased threats to staff engaged in sensitive work, embarrassment or damage to participants, benefactors and suppliers

11. Storage And Backup

It is the responsibility of each person to ensure sensitive data is stored, secured and backed up as per the required schedule. All sensitive data must be stored and secured via the approved and provided electronic/physical storage locations.

12. Data Anonymization

All appropriate steps must be taken prior to disclosing, sharing, or transferring information to ensure the anonymity of a data subject is undertaken and maintained in accordance with the appropriate legislation.

Omitting/Redacting

Omitting or deleting specific personal identifiers is the most basic privacy method whereby sharing or releasing information removes personal data from any documents/records including omitting and redacting sensitive data.

Audio-Visual/Verbal Exchange

Audio-visual data and/or participant information can be difficult to anonymise due to the nature and format of the recordings. Audio-visual and verbally exchanged recordings, where required, should be masked, edited and/or dubbed.

13. Secure Disposal

Information assets that are considered sensitive (i.e. Secret, Strictly Confidential or Confidential) and are no longer needed or are deemed to have reached “end of life” must be securely disposed of. There are several

ways to dispose of information assets and equipment. For example: secure shredding (cross cut shredders).

14. Information Security Incident Response

In the event that an information asset is damaged or lost, this must be reported immediately to the appropriate manager and to your relevant Information Security Manager.

End.