DIGITALPOWER UK LTD

Information Classification Policy

Table of Contents

Information Classification Policy

1. Purpose

The Information Classification Policy is applicable to Digital Power UK Ltd. This policy recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its interested parties.

The Information Classification Policy forms a key control to ensure that the confidentiality, integrity and availability of our information assets, are protected effectively and that we can meet our obligations to the interested parties and is applicable for all assets within the scope of the System Architecture ISMS used by Digital Power UK Ltd.

2. Scope

The Information Classification Policy applies to all information assets created held and processed on behalf of Digital Power UK Ltd and will be categorised by Digital Power UK Ltd Incident Security Classification Scheme, this will be based on the risk posed to the data being processed, transmitted, accessed or modified by an unauthorised party.

3. Policy Statement

The Information Classification Policy aims to provide the necessary guidance to classify an information asset, and how that asset should be handled throughout its lifecycle. The scheme aims to mitigate the risk of the information asset being compromised by taking a risk-based approach for implementing controls which are deemed adequate and proportionate to the organisation's appetite for risk.

The Information Classification Policy defines the categories of classification that information can fall into, and how data will be handled with respect to each category to preserve the Confidentiality, Integrity and Availability of information assets.

Information can take many forms including, but not limited to:

- hard copies of data held on paper;
- data stored electronically in computer systems;
- communications sent by physical post or using email; and
- data stored using electronic media such as USB Drives, disks and tapes.

On creation, all information assets will be assessed and classified by the owner according to its content. The classification, when correctly assigned as per Table 1 - Classification Impact Statements is based on impact of loss, modification or exposure of assets, and will determine how the information is labelled and thus throughout its lifecycle how the asset(s) are protected, stored, transferred and deleted.

The Digital Power UK Ltd Information Security Classification Policy requires information assets to be classified into one of four classifications:

- Level 0 – Public (or unclassified)
- Level 1 – Protected
- Level 2 – Restricted
- Level 3 – Confidential

3.1 Security Classifications

The Security Classifications are described in further detail below. The following criteria shall be considered when deciding which classification an information asset should fall into based on impact of loss of 1 or more of Confidentiality, Integrity and/or Availability:

- Legal requirements
- Value to the organisation
- Criticality to the organisation
- Sensitivity to unauthorised disclosure or modification

These areas are considered against the classification impact statements below:

Classification	Primary Impact Statement	Comments
Public	Public information is information which would not violate any laws or regulations such as privacy rules in its publication, neither would it cause Digital Power UK Ltd to come into disrepute or lead to financial loss. Public information can be disclosed without any restrictions on the content or audience.	Digital Power UK Ltd information is classified as Public is freely available to the public; however, it is necessary to maintain an awareness of any information that falls within the 'public' classification as change of circumstances may evoke the need for a revised security category.
Protected	Protected information is information which would have undesirable consequences if lost or disclosed to unauthorised parties, however it will not result in significant negative consequences.	Most Digital Power UK Ltd employees will handle Protected Information throughout the course of their working day. Examples of Protected Information are invoices, backing data for supplier invoices, expense claims and mileage reports and encrypted data.
Restricted	Restricted Information is information that would have a more serious detrimental effect if it is lost or disclosed to unauthorised parties. If could result in significant reputational damage or financial loss to Digital Power UK Ltd and may lead to legal consequences.	Restricted information will be distributed on a 'need to know basis,' and will typically be handled by middle management and above, although employees at a lower level may be given access as required. Examples of Restricted Information are supplier information i.e. customer and non-sensitive personal information.

Confidential	Confidential information is restricted to information that is highly sensitive and would cause major reputation and financial loss if it were lost or wrongly disclosed, it could also lead to legal consequences.	Access to Confidential Information assets will be tightly controlled by senior management and paper copies will be numbered and distributed according to specific procedures. Examples of Confidential Information are employee details and contracts, supplier contracts and prices charged for products and services, sensitive customer information, Digital Power UK Ltd payment information and bank details, I.P. Addresses, Private Keys, Passwords, Shared services data.

Table 1: Classification Impact Statements

3.2 Owner Management

When deciding how to categorise information the owner of the document should ensure that only genuinely sensitive information is subject to additional controls.

It should be considered that applying too high a classification could inhibit access, lead to unnecessary and expensive protective controls and impair the efficiency of Digital Power UK Ltd's business. Alternatively, applying a classification that is too low may lead to damaging consequences through compromise of the asset.

Security Classification of assets and documents should be reviewed at the time they are created, and after any further amendments in case classification has changed due to change in content, business requirements, or regulatory requirements.

When considering how to classify an asset into any of the four categories above, the information owner should consider the effect unauthorised disclosure would have on the following:

- Cause distress to individuals
- Undermine undertakings to maintain confidence of information provided by 3rd parties
- Breach statutory restrictions on disclosure of information
- Cause financial loss or loss of earning potential
- Give an unfair advantage to individuals or parties
- Prejudice the investigation or facilitate the commission of crime
- Disadvantage the organisation in commercial or policy negotiations
- Impede the effective development or operation of organisational policies
- Undermine the proper management of the organisation and its operations

As a minimum where an unauthorised disclosure may have the potential for any of the consequences below then they should be immediately considered as having a classification of Confidential until such time evidence is provided that downgrades this assertion:

- Significantly materially damage relations with organisations (e.g. formal protest or other sanctions)
- Prejudice individual security or liberty
- Cause damage to the operational effectiveness or security of Digital Power UK Ltd
- Work substantially against organisational finances or economic and commercial interested
- Impede the investigation or facilitate the commission of serious crime
- Substantially undermine the financial viability of major organisations
- Shut down or otherwise substantially disrupt significant business operations

The lists given above are provided as guidance and are non-exhaustive. It is up to the information asset owner's discretion and responsibility if they believe the data should be assigned a higher or lower

classification. At all times where there is doubt then asset owners should seek guidance in the first instance from the Digital Power UK Ltd security Officer.

3.3 Security Controls and Handling Requirements

Table 2 defines the handling measures that should be taken when storing, processing, transporting and/or deleting assets created or held by Digital Power UK Ltd, and applies to both electronic and paper forms of assets.

In addition to accurately classifying single instances of assets, consideration should be given to the additional attraction to unauthorised users when assets are aggregated and there is likely to be an increase in the volume of the data sets of information.

Larger data sets of information of the same classification are likely to attract a higher impact (particularly in relation to personal data) than that of a single instance. Generally, this will not always result in a higher classification but may require additional handling arrangements due to the increase in impact of loss.

However, if the accumulation of that data results in a more sensitive asset being created, then a higher classification should be considered and applied using the guidance within the document.

Security Control Category	Data Classification			
	Public	Protected	Restricted	Confidential
Copying / Printing (applies to both paper and electronic forms	No restrictions	Data should only be printed when there is a legitimate need	Data should only be printed when there is a legitimate need Data should not be left unattended on a printer/scanner. Copies must be labelled "Restricted"	Data should only be printed when there is a legitimate need Copies should be numbered. Data should not be left unattended on a printer/scanner Copies must be labelled "Confidential" with names of those who have been granted access
Labelling	Do not need to be labelled	Do not need to be labelled	Copies must be protectively marked with the label of 'Restricted'	Copies must be protectively marked with the label of 'Confidential' and include a distribution list of

				those who have been granted authorisation to view the document
Access	No restrictions	Limited to Digital Power UK Ltd Staff	Limited to individuals with a 'need to know'	Copies must be limited to named individuals authorised to access the data. A confidentiality agreement may be required.
Virtual Environments	May be hosted in a virtual environment	May be hosted in a virtual environment	May be hosted in a virtual environment with clearly documented controls for implementing and managing separation.	May be hosted in a virtual environment with clearly documented controls for implementing and managing separation.
Physical Security	System must be locked or logged out when unattended	System must be locked or logged out when unattended. Access only available through key fob out with working hours.	System must be locked or logged out when unattended Access only available through key fob out with working hours . Access is arranged on a Need to Know basis. Unauthorised users are escorted.	System must be locked or logged out when unattended Access only available through key fob entry named, individuals only Access is arranged on a Need to Know basis. Unauthorised users are escorted.
Data Storage	Should be stored on a secure server.	Should be stored on a secure server. Paper/Electronic Media: do not leave unattended	Should be stored on a secure server. Work should not be stored solely on a single individual's device. Restricted documents should	Should be stored on a secure server. Work should not be stored solely on a single individual's device. Confidential

		where others may see it.	be saved in a User Restricted 'need to know' folder as determined by Digital Power UK Ltd Paper/Electronic Media: do not leave unattended where others may see it; store in a secure location such as locked cabinets with the distribution of keys limited to those who require access and have been granted permission by the document owner to view the document.	documents should be saved in a User confidential 'need to know' folder as determined by Digital Power UK Ltd Encryption on backup media required Paper/Electronic Media: do not leave unattended where others may see it; store in a secure location such as locked cabinets with the distribution of keys limited to those who require access and have been granted permission by the document owner to view the document. Cryptographic material: Should be stored in a cryptographic module of at least FIPS140-2 level 2 or equivalent, Where necessary cryptographic material can also be stored on a USB stick in encrypted form in a locked cabinet.
Data Transmission	No precautions are required	Internal Email: Through the internal email system. The receiver should have a business	Internal Email: Through the internal email system. The receiver should have a business	Internal Email: Through the internal email system. The receiver should have a business

		requirement to have access to the document. External transfer should be as Secure File Transfer Protocol	requirement to have access to the document. External transfer should be as Secure File Transfer Protocol	requirement to have access to the document. External transfer should be as Secure File Transfer Protocol
Transporting Physical Assets **Electronic, and paper**	No precautions required	To be sent by signed and tracked delivery Cryptography should be used to protect data on a USB stick. PIN/Password should be sent separately	To be sent by a reliable and trusted courier. Signatures are required on receipt. Cryptography shall be used to protect data on authorised and controlled USB media device using. PIN/Password sent separately via email.	As far is possible data should be delivered by Digital Power UK Ltd staff with signature on receipt. Otherwise only to be sent by a reliable and trusted courier. Envelope must be labelled 'Confidential' Cryptography should be used to protect data on USB stick. PIN/Password should be sent separately via email.
Disposal of paper information (the document owner is responsible for destruction when copies	Paper recycling	Cross-Cut Shredder and recycled	Cross-Cut Shredder and recycled	Cross-Cut Shredder and recycled.

are no longer required.)				
Erasing Electronic Data	'Deleting' is sufficient	Deleted using Disk-Wiping Software "Active KillDisk Ultimate" or equivalent	Deleted using Disk-Wiping Software "Active KillDisk Ultimate" or equivalent	Deleted using Disk-Wiping Software "Active KillDisk Ultimate" or equivalent
Disposal of Electronic Media	Physical device appropriate environmentally friendly disposal	Secure destruction required as set out in Physical Security Policy	Secure destruction required as set out in Physical Security Policy	Secure destruction required as set out in Physical Security Policy. It is at Digital Power UK Ltd discretion whether staff should be witness to destruction. If so, a minimum of two staff should be witness. Destruction of cryptographic material should be undertaken by decommissioning the device and destroyed as per Physical Security Policy

Table 2: Handling controls for determined classified data

4. Change Control

This Policy document will be formally controlled and used as the basis for monitoring and measuring compliance of Information Classification processes and procedures.

Any changes to this policy shall only occur after completing a risk assessment against the changes for Digital Power UK Ltd, and its effected customers.

Any material changes should be made by adhering to the latest Change Management Policy.

Consequences

Non-compliance with this policy could have a significant effect on the efficient operation of the organisation and may result in financial loss and an inability to provide necessary services to our customers. If any employee is found to have breached this policy, they may be subject to disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).