



**DIGITALPOWER UK LTD**

## Data Retention Policy

## Table of Contents

Insert logo .....	1
Digital Power UK LTD .....	Error! Bookmark not defined.
<b>1. Purpose.....</b>	<b>3</b>
<b>2. Scope .....</b>	<b>3</b>
<b>3. Policy Statement .....</b>	<b>3</b>
3.1 <i>Definitions</i> .....	3
3.2 <i>Roles and Responsibilities</i> .....	4
3.3 <i>Aims of the policy</i> .....	4
3.4 <i>Determining Data Retention</i> .....	4
3.5 <i>Recommended Retention</i> .....	4
<b>4. Policy Change Control .....</b>	<b>5</b>
<b>Consequences .....</b>	<b>5</b>

# Data Retention Policy

## 1. Purpose

The Data Retention 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 Data Retention 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 used by Digital Power UK LTD.

## 2. Scope

Digital Power UK LTD will be storing large quantities of data on its System Architecture, and the secure handling, retention and protection of this data is necessary in order mitigate any risks pertaining to the data held therein as identified in Digital Power UK LTD Risk Assessment.

This policy will set out a framework for which Digital Power UK LTD will govern decisions on whether data should be retained or disposed of; dependent on the data classification defined in the Information Classification Policy, any relevant regulatory compliance, and the practicalities of storing data for long periods of time.

The method for storage, protection and disposal is set out in Information Classification Policy

All data and information assets handled and stored by the IT User systems will be retained in accordance with this policy.

## 3. Policy Statement

Digital Power UK LTD with support from Data Management will ensure information is not kept longer than is necessary and will retain the minimum amount of information that is required to maintain provision of the IT User System to its Service Users whilst continuing to fulfil its regulatory requirements.

Erasure or disposal of data will be dependent on the nature of the information asset and the Asset Register should detail the length of time data will be retained.

### 3.1 Definitions

Word/Phrase	Definition
<b>Online</b>	Data is accessible without request.
<b>Archive</b>	Data is accessible only by request and will require a period of time to provide access.
<b>Remove</b>	Deleted from the Shared Services system and archives, no longer accessible, restorable or recoverable.
<b>Static Data</b>	Collection of data in memory that is fixed in size. Thus, maximum size of data is known in advance. E.g. Static tables, static market data

### 3.2 Roles and Responsibilities

Role(s)	Responsibilities
<b>Asset Owner</b>	Responsible for determining (in accordance with this Policy) data retention for the asset. The operational aspect of this function can be delegated to another Shared Services staff member.
<b>IT Support</b>	Erasure of electronic data when determined by the Asset Owner. (Erasure should be completed in accordance with Information Classification Policy)

### 3.3 Aims of the policy

The following considerations should be taken into account by the Asset Owner to ensure that personal data that we hold is kept secure and that it is held for no longer than is necessary for the purposes for which it is being processed. In addition, we will retain the minimum amount of information to fulfill our statutory obligations and the provision of goods or/and services - as required by the data protection legislation, including the UK General Data Protection Regulation (UK GDPR).

### 3.4 Determining Data Retention

The following considerations should be taken into account by the Asset Owner when determining the retention period of data:

- The classification of information as given in Information Classification Policy
- Whether retention is required to fulfil statutory or other regulatory obligations.
- Whether retention may be required for evidence throughout incident investigation or legal proceedings.
- Whether retention is required to meet the operational needs of Shared Services.
- A guide to the recommended and statutory minimum retention periods for specific data is given in section 3.5 Recommended Retention

Asset Owners should assign data retention for an asset following an assessment of the risk posed. This will ensure that the measures in place are proportionate to the risk of no longer having access to that asset and(or) unauthorised disclosure of the data.

### 3.5 Recommended Retention

The following table gives a guideline to the Asset Owner of retention periods for data. This table is redundant in any cases where it is overridden by regulatory requirements.

Data Retention Requirements			
Function	Online Retention	Archiving Retention	Removal
<b>Static Data</b>	Kept online indefinitely	N/A	N/A
<b>Appointment and Site Data</b>	40 months after the end of appointment	41 - 84 months after the end of appointment	85+ months after the end of appointment
<b>Consumption Data</b>	40 months	41 – 84 months	85+ months
<b>Audit Data</b>	For previous and current audit year	N/A	After 2 Audit Years
<b>Service Request Data</b>	40 months	41 – 84 months	85+ months

#### **4. Policy Change Control**

This Policy document will be formally controlled and used as the basis for monitoring and measuring compliance of Data Retention 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).