Backup Policy

Purpose

This document outlines the policies in place for the provision of backing up data within the company for all departments.

Backup Strategy

There are 5 key types of data that are considered within this policy namely:

- Company design data
  - This is data containing the drawings and source code used to produce and operate Instrumentel's products
- Required contractual information
  - This is documents that are creating for each project
- Customer derived data (including asset raw data)
  - This is data collected from customers. Either directly from the customer or Instrumentel's hardware installed on the asset.
- Server Systems
  - This is the operating system data as well as any configuration data used to run Instrumentel's core operations.
- Security Keys and logins
  - Any secrets used to authenticate Users and/or services either from a Instrumentel system as both a first party or third-party system.
  - Any secrets also used to encrypt and secure any data that Instrumentel accesses.

Local data

All data and information that is created on workstations is to be stored within the repository specific to that project or element at the end or each day (minimum). On commission to the repository, data is to be labelled with appropriate descriptive information so that it can be reverted back to if necessary (examples include Firmware revisions, PCB design files etc).

Only work-related documents and programs should be maintained on any workstation and under no circumstance should work related information be stored on a personal device without prior consent from a line manager.

Backup Intervals and Retention Periods

Company Design Data and Required contractual information

Design files are backed up at weekly intervals held for a month, and monthly snapshots held for 6 months.

Customer derived and Asset Data

Asset Data are backed up weekly. The retention period of data will vary depending on the contractual agreements per project.

Server Systems

Monthly snapshots are taken weekly and held for a minimum of 6 months.

Security Keys and logins

Security files are backed up at weekly intervals held for a month, and monthly snapshots held for 6 months.

Backup Location

There shall be at least one local copy and another offsite. This ensures there are 2 venues to access data in case any-one venue is inaccessible.

Backup Security

All data held offsite will be encrypted both at rest and in flight to ensure data security. The keys for this data will also be backed up and only accessed by authorised personnel.

Asset data

Asset data is gathered from many units that are out in service, the rate at which the data is gathered will be application specific and all data is to be stored on the production server in the first instance. This production data will be then backed up to two separate locations.

Data backup procedure

Data will be backed up on routine specified above. Each snapshot will be appropriately timestamped. These snapshots are removed inline with the retention period specified that that data type.

A log of the backed-up data will be maintained as an output for each backup run. All sensitive data will be indicated as such and will be encrypted to ensure no non-authorised usage.

Data recovery

To recover from an instance of service or data loss, the data affected can be restored to its last backup snapshot. Any hardware or service migration may need to occur during any severe hardware or service outage. Hardware and data will then be checked for its integrity before being signed off to resume service. Confirmation of the data recovery should be indicated to all manger level members of staff.

Data recovery Drills

Data recovery will be practiced every 6 months. Data loss will be simulated through the need of having to replicate part of the Instrumentel's digital service. This will validate that data is up to date, is fully intact and captures everything needed to restore the digital service.

These drills will be timed to monitor potential impact of how long a system will take to restore. Aiming for a full rebuild of the targeted part to take less than 24 hours.

Key Contacts

The main contacts listed for this policy are:

Jonathan Birch – Technical Manager
Lee Barker – Firmware Team lead
Satyaranjan Thumma – Dev Ops Engineer

Applicability

This policy is applicable to all company employees and all official corporate records.