SECUREDRIVES

DSPS
DATA SECURITY PROTOCOL SWITCH

The Data Security Protocol Switch gives you the ability to physically destroy up to fifty SDSDSP solid-state disk drives instantly from a single point of command.
This is an effective 'kill switch' designed for governments or organisations operating in potentially hostile locations where instant data destruction is required in cases of emergency.

The DSPS offers:

- Single point of reference / command
- Instant data destruction for an office of computers
- Centralised control of up to fifty SDSDSP hard drives
- **Dual button & key activation** - safeguards against accidental activation
- **Signal Proximity** - protects against computer theft and signal starvation
- **Battery backup** - safeguards against mains power sabotage
- **TPM encrypted communication** - safeguards against a 3rd party signal

A unified approach to data security

www.securedrives.co.uk

SecureDrives – Security by design

SECUREDRIVES

Data Security Protocol Switch

Power Supply

- Micro USB 2.0 mains power
- Battery backup (30 days autonomy)

Interfaces

- Capacitive touch screen
- Dual button destruction with master key

Communication

- Trusted Platform Module via ANT

Compatibility

- Supports internal & externally deployed SDSDSP hard drives
- Supports 64GB & 128GB SDSDSP capacities

Assignment capacity

- One to fifty SDSDSP drives

Resilience

- Two DSPS's can be deployed in one room
- Allows two points of control
- Delivers hardware resilience

Zoning

- More than one DSPS can be deployed
- Facilitates grouping of computer drives to specific DSPS's

Signal Proximity

- Protects against hard drive theft
- Protects against signal jamming

Setting a new bench mark for security of Data-at-Rest

- Single point of command, the DSPS allows instant destruction of up to fifty computers simultaneously
- Ideal for offices in potentially hostile environments where sensitive data needs to be protected from unauthorised access in times of emergency
- Instant data destruction without complex authentication processes allows security protocols under duress situations to be concluded efficiently
- Signal Proximity (SP) option provides a safeguard against theft. If a hard drive or computer with a hard drive installed is removed from the proximity of its assigned DSPS, the hard drive will self-destruct
- The Signal Proximity option provides safeguards against signal jamming. If the SDSDSP hard drives can't hear the DSPS for a given period of time (user defined) the hard drives will assume this is a an attempt to gain unauthorised data access and will self-destruct
- The unique DSPS case requires a master switch key followed by a double button press to activate the destruction and therefore protects against accidental activation
- Up to two DSPS's can be deployed in the same room controlling the same computers. This delivers multi points of command and hardware resilience if required
- Multiple DSPS's can be deployed for zoning. Allowing specific computers to be assigned to specific DSPS's. Each DSPS can be named (shown in the display) to facilitate easy identification
- Battery backup means the DSPS remains operational in the event of mains power failure / sabotage. All SDSDSP drives are battery supported allowing the complete data security solution to be independent of mains power
- TPM (Trusted Platform Module) secures the communication between the Data Security Protocol Switch and the SDSDSP hard drives safe guarding against any 3rd party signals
- Easy assignment of new SDSDSP hard drives and un-assignment of existing hard drives are made via the DSPS GUI