

Accounting / Administrative

KIP Data Security Features

At KIP, security is paramount. As a world leader in the development of digital wide format production technology, KIP is committed to keeping digital information safe and secure. Customers and potential customers can look to KIP as a trusted provider of secure solutions with many standard and optional security features.

Based on Department of Defense NISPOM specifications, the Image Overwrite security feature electronically shreds information stored on the hard disk as part of routine job processing.

Job Accounting and Data Tracking ensures that only properly authorized users are permitted to use a KIP device. Two additional fields, displayed in each KIP application can enforce tracking by Project or Department Number. These standard features feed the KIP Cost Center to generate production reports based on User, Project or Department usage.

Eliminate the risk of unauthorized access with the optional Removable Hard Disk Drive kit. The removable hard drive can be disconnected when the device is unattended. Multiple disk drives can be implemented allowing secure device sharing between different workgroups or departments. This option is frequently required by the US Government for management of classified information and highly recommended for commercial customers who print data that is subject to legal regulations including HIPAA, SOX and PCI.

The System K controller is designed and constructed to utilize standard open architecture PC components. KIP printing speeds and unique image processes are supported by the KIP System K Controller with Microsoft® IoT Enterprise embedded operating system. The Microsoft® partnership with KIP ensures an industry standard that provides excellent reliability.





KIP Data Security Key Features



Image Overwrite | Removable Hard Disk Drive Accessory Kit | KIP System K Controller with Microsoft® IoT Enterprise Embedded Operating System | Standard Security Updates | Data Encryption and Virus Scanning Applications | KIP Secure Print | KIP Accounting Center Integration | KIP Cost Center Integration



Image Overwrite

Electronically Shreds Copy, Print and Scan Data | Standard Feature | Automatic Deletion | 3 – Pass Erasure Algorithm | Configured via Printpro.net | Based on NISPOM 5220.22-M Requirements



Removable Hard Disk Drive Kit

Share KIP Device between Secure Workgroups and Departments | Remove External Hard Disk Drive as Required | Additional Disk Drives Available | Management of Classified or Legally Restricted Data | Separate Usage for Confidential and Non-Confidential Work



Job Accounting and Data Tracking

Access Control | User Authentication | Project Number Authentication | Scan/Print Authentication at Touchscreen | Scan/Print Authentication in KIP Software Apps | KIP Accounting Center Integration | KIP Cost Center Integration



Windows® Operating System

Microsoft® Windows Embedded Partner | Accepted by IT Managers | Start Up and Shut Down Quickly | Improved Memory Utilization | Accepts Automatic Updates | Configure Microsoft® Management Console to Update via WSUS



Data Encryption and Virus Scanning

Data Encryption via SSL and IP Security (IPSec) | Major Brands Tested | Accepts Virus Definition Updates



KIP Secure Print

Confidential Printing | Unique 4 Digit Security PIN | Jobs Print when Released by User | Reduce Waste – No Uncollected Jobs | Standard Feature in all KIP Software Apps | Secure PIN from Smart Print via Email