

# Document Security Solutions for Manufacturing

## Increase Document & Data Security Security Tips to Protect Network Devices & Business Data

Document Software Solutions can help your manufacturing business by helping to protect your sensitive and private documents and data. Not only can they efficiently store, manage, access, and distribute enormous volumes of information, but they also safeguard business documents and data with a series of controls and security efforts.

When it comes to security on Multi-Functional Devices – MFD's and Multi-Functional Printers – MFP's, all organizations need to ensure that they can securely manage any network device to defend off hackers and protect their stored data. It's critical to protect your corporate documents and data throughout your workflow, from the data traveling through your network to the pages landing in your output tray. These security measures need to be securely accessible and able to be remotely managed.

**1. Automatic Data Backups** – Nothing is more valuable than the data that drives your business. And nothing is more critical than backing up key systems and databases. Document Software Solutions can provide automated backup of critical files and data. They can also enable automated disaster recovery so that you can bring your systems and data back online in a quick and efficient manner. Document Software Solutions are affordable and will periodically back up your files at regular intervals, eliminating manual backups which can be unreliable.

**2. Data Encryption** – MFP/D's can encrypt data that is carried on the network to and from the devices to prevent unauthorized access to documents as they travel to file servers or other network servers. When storing scanned data as a PDF file, the data can be encrypted. In order to open the PDF document file with Adobe Acrobat, it is necessary to input a security code to decrypt the document.

**3. Password Protection** – One of the top priorities of any IT Manager is to ensure only authorized persons are accessing the appropriate devices and data within an organization. By utilizing user logins and passwords or Security ID Cards, network authentication can restrict workers' access to scan, email and fax functionality as needed. Customized security plans may be needed for networked MFP/D's to protect each user's data from unauthorized access by other users.

Data access security breaches can happen at unexpected times and in unexpected ways. In order to help prevent sophisticated security attacks, it's important to keep documents and data safe during all aspects of data transfer between paper and digital formats.

### 4. Track and Monitor Who Accesses, Changes and Deletes Files

– Within the document management workflow processes, there are numerous ways to electronically track and monitor the individuals that can access secure documents and data within an organization.

- Internal audit log — MFP/D systems can maintain audit logs of activity to help track the routing of documents. This can be especially beneficial for organizations that must comply with federal regulations.
- Firewall — This enables MFP/D's to manage all data transfer access to only those that are authorized users.
- Secure Print — This feature allows MFP/Ds and users to hold print jobs in the queue until they physically arrive at the device and enter a password or code to access the document or print it. This prevents unauthorized viewing of documents as they wait in the output tray.
- Document Version Control — Nothing is more frustrating than looking for the original document after it has been modified; one, two or three plus times. Keeping track of those versions as well as who did those modifications is particularly important now more than ever.

Security threats are very common and on the rise. And in most manufacturing companies, the effect of such a breach can be utterly detrimental to the health or even survival of the organization. The result can mean that unauthorized individuals can gain access to private or highly sensitive information and data. In a data-driven world, corporate information is just too lucrative and too easy to steal.

Call James Imaging Systems today for your free, no obligation Document Management Needs Assessment!

