DEVELOP

Dynamic balance

www.develop.eu

Security you can count on

Develop's security standards

In today's business company data have to cross a lot of different data highways. Nearly every work process and workflow starts, ends or is somehow related to your multifunctional office device. A lot of your business data is running through your ineo system. This is the reason why, as a main element of your business work processes and workflows, your office device has to withstand ongoing threats to security.

Develop systems are certified, almost without exception, in accordance with the ISO-certified Common Criteria requirements 15408/IEEE 2600.1. These are the only internationally recognised standards for IT security testing for digital office products. Once certified, the devices will have passed a strict security evaluation and be able to satisfy and deliver the kind of security levels that a prudent business operation should look for and rightfully expect.

DATA SECURITY

Access control/access security

The features available on these multifunctional systems are easy to operate. The first logical step is to prevent unauthorised persons being able to use the system. This is why authentication is needed, and should include the definition of users and user groups as well as limitations to access and usage rights. DEVELOP provides a variety of technologies to protect your data – a personal password, ID card & mobile authentication, and a biometric finger vein scanner.

Data security/document security

When the multifunctional system is located in a public area, confidential data can be accessed by staff, contractors or even visitors. These data may be available via printouts lying in the output tray or stored on the system's hard disk. For this reason it is important to implement security policies that guarantee that the documents and data will not leave your company. DEVELOP's comprehensive security functionality, e.g. HDD encryption and HDD password protection, secures user details and output content, helping to prevent sensitive corporate information from falling into the wrong hands.

Network security

Today's business environment is characterized by connected systems, automatic data collection and transmission to downstream systems that subsequently handle the data. DEVELOP office devices are designed to work in network environments, enabling fast processing workflows with the ability to scan data to network destinations or receive print jobs from different devices and destinations.

This complies with strict security standards on user access, encryption of data and protocols used for information transmission so you can ensure your data will arrive at the desired destination in a secure and trustworthy manner.

DEVELOP security functions at a glance

Access control

- User authentication (ID card, mobile device, password)
- Finger vein scanner
- Function restriction

Data security

- Data encryption (hard disk)
- Hard disk data overwrite
- Hard disk password protection
- Data auto deletion
- Secure printing (lock job)
- Copy/print accounting
- User box password protection

Network security

- IP filtering
- Port and protocol access control
- SSL/TLS encryption (HTTPS)
- IP sec support
- S/MIME
- 802.1x support

Scanning security

- User authentication
- POP before SMTP
- SMTP authentication (SASL)
- Manual destination blocking

Network security

- Service mode protection
- Admin mode protection
- Data capturing
- Unauthorised access lock
- Copy protection via watermark
- Encrypted PDF
- PDF signature
- PDF encryption via digital ID
- Copy guard/password copy

DEVELOP