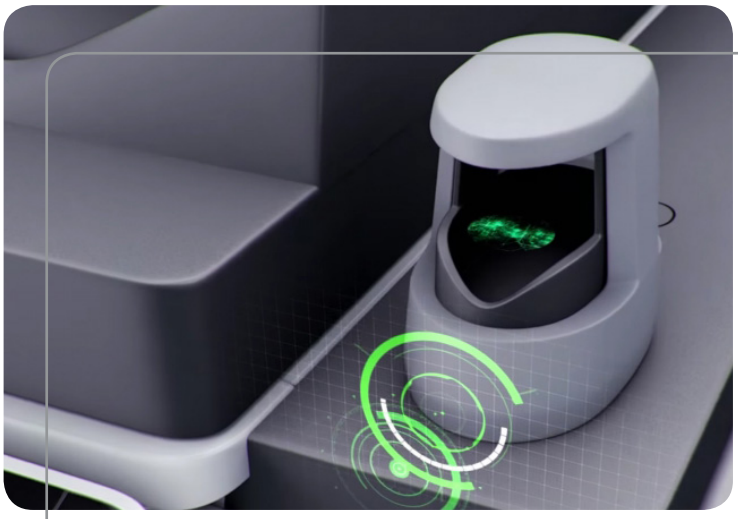
GO FOR INDUSTRY-LEADING STANDARDS:
RETHINK PROTECTION

ITEC SECURE
PROTECT PRINT SMARTER



NO MORE **LOOPHOLES**

Rethink Document & Data Security

It is important to be aware of the fact that today no enterprise is immune to security risks – security breaches happen everywhere, all the time! However, prudent company owners plan ahead and take the necessary precautions before the attack.

By partnering with Itec, the pioneer and industry leader in this field, you are taking advantage of the comprehensive range of security features available for our Itec MFPs and Lexmark printers.

Conscientious managers understand that MFPs and printers installed throughout their company can constitute the most serious of security gaps. If left unattended in the output tray, confidential information might get into the wrong hands and easily leave the company, for example via scan-to-email or fax transmission.

ISO 15408 Certification

Itec devices are certified almost without exception in accordance with the Common Criteria ISO 15408 framework. These are the only internationally recognised standards for IT security testing for digital office products. Printers, copiers and software compliant with Common Criteria certification have all passed a strict security evaluation and are able to satisfy and deliver the kind of security levels that a prudent business operation seeks.

As a security-conscious company owner or manager, you will want to ensure that your network is protected and that unauthorised access to information on the company's intranet is blocked. At Itec, we support your efforts to protect against security risks by allocating extensive engineering resources to the advanced development of security-related features for our Itec MFPs and Lexmark printers. Providing our customers with the latest technology required for today's security-conscious environments, we create industry-leading standards, thus offering you the level of comprehensive protection that our customers from all industries and public authorities rightfully expect.

Lexmark™ ITEC

Whether you are concerned about network intrusion, data theft or compliance with regulations, or your focus is on limiting access to devices or functionalities, the innovative technology in our Itec MFPs and Lexmark printers includes professional solutions for the detection and prevention of security breaches.

DOCUMENT AND DATA SECURITY

Beware of unauthorised access to MFPs installed in public areas – implementing appropriate data security policies is essential here. After all, sensitive data stored on the MFP hard disk over a period of time as well as confidential prints left in the MFP output tray are not protected and might easily fall into the wrong hands. Itec offers a comprehensive range of tailored security measures to curb any such attempts and ensure complete document and data security.

Countless MFPs and printers are located in public areas without restricted access. This makes the implementation of an appropriate data security policy essential. To avoid critical information falling into the wrong hands, Itec offers various security measures that ensure complete document and data security.

Smart PDF Encryption

Encrypted PDFs are protected by a user password: Permission to print or copy the PDF and permission to add PDF contents can be configured during the scanning phase at the MFP.

PDF Digital Signature

This useful feature adds a digital signature to the PDF during scanning and thus allows monitoring any changes to the original PDF content.

User Box Security

Available for single users and groups, user boxes allow for any document to be securely stored on the MFP hard disk before output of the print or copy job. They are protected with an eight-digit alphanumeric password that needs to be entered to access/ view the documents in the box.

Secure Fax Reception

When activated, any faxes received are kept safe in a protected user box.

HDD/SDD Encryption

HDDs/SDDs in Itec devices can be encrypted using the Advanced Encryption Standard (AES), supporting a 256-bit key length and satisfying corporate data security policies. After encryption, the data cannot be read or retrieved, even if they are physically removed from the MFP.

HDD/SDD Security

Hard disks and memory on MFPs retain many gigabytes of confidential data collected over long periods. In Itec systems, a number of complementing features ensure the safekeeping of such sensitive corporate information.

SECURE PRINT

There is no easier way for anyone unauthorised to gain access to confidential information than grabbing it lying unattended in a printer output tray. The secure print feature ensures document confidentiality by obliging the print originator to protect the print file with a password and entering this at the output device immediately before printing.

ONLY AUTHORISED COPYING

The copy protection feature adds a watermark to prints and copies during printing. Hardly visible on the original print, the watermark moves into the foreground on any copy of the original document.

PRINTING WITH INDIVIDUAL AUTHENTICATION

Touch & Print needs authentication via finger vein scanner or ID card reader while ID & Print requires user authentication via ID and password. The print job is output only after the user has thus authenticated at the MFP. The advantage here is the speed: there's no need for additional security print ID and password.

CONTROL VIA COPY GUARD

With Copy Guard/Password Copy, a concealed security watermark is added to an original print to prevent this from being copied. While barely visible on the protected original, the security watermark blocks Itec devices from copying such documents. Only the Password Copy feature can override Copy Guard and allow copies to be made when the correct password is entered at the MFP panel.

- **AUTO DELETE** - Data stored on the hard disk are automatically erased after a set period.
- **HDD/SDD PASSWORD PROTECTION** - Any read-out of data stored on the hard disk requires password entry, with the password linked to the device. Data are therefore no longer accessible once the HDD/SDD is removed from the device.
- **HDD* OVERWRITING** - The most secure method of formatting a hard disk is by overwriting stored data. This is performed in accordance with a number of different methods conforming to various (e.g. military) specifications.

ITEC
QUALITY PEOPLE, SMART TECHNOLOGY SOLUTIONS

+27 11 236 2000 • info@itecgroup.co.za • www.itecgroup.co.za

MANAGED
BUSINESS SERVICES