ITEC SECURE

GO FOR INDUSTRY-LEADING STANDARDS:
RETHINK PROTECTION

ITEC SECURE
PROTECT PRINT SMARTER

PROTECT COMMUNICATION **INSIDE & OUT**

Rethink Network 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.

NETWORK SECURITY

Within your corporate network, our printers and MFPs act as sophisticated document processing hubs that scan, print and copy documents to network destinations, or send data via email. Office technology from Itec is subject to the same security risks as any other networked device. Which is why we ensure that all our equipment complies with the strictest security standards and offers multiple features against potential security leaks that might attempt to use your network connection.

Itec's office devices are based on a concept of communication and connectivity. This complies with strict security standards concerning user access, encryption of data and protocols used for information transmission. Trust us to ensure that your data will get to the desired destination securely and will not be tampered with.

USER AUTHENTICATION

Besides governing access to output devices, the need to authenticate with a unique user ID and password prevents unauthorised users from accessing the network. The feature can be configured to authenticate to the network or directly at the MFP or printer.

IP ADDRESS FILTERING

An internal basic firewall provides control of protocol and port access as well as IP address filtering, which can be set at the machine: the MFP's network interface card is programmed to only grant access to a specific IP address range from client PCs.

SECURED PORTS AND PROTOCOLS

In the administration mode at the machine or remotely via Web Connection or Device Manager, ports and protocols can be opened, closed, enabled and disabled. The administrator mode itself is accessed by a 16-digit alphanumeric password that can only be changed by the service engineer or administrator. If required, a web interface closing functionality also allows the disabling of the web interface for all users.

SSL/TLS ENCRYPTION

It protects communication to and from output devices, covering online administration tools, the Enterprise Server and Active Directory transmissions, etc. This communication type prevents from man-in-the-middle attacks where the attacker would be able to record the data communication.

IPsec

Itec devices support IPsec for the complete encryption of any network data transmitted to and from the MFP. The IP security protocol encrypts the entire network communication between the local intranet (server, client PC) and the device itself.

SMTP AUTHENTICATION

Ensuring advanced email security, SMTP authentication (Simple Mail Transfer Protocol) will authorise a machine to send email when activated. Companies not hosting their email services can use an ISP mail server. For secure communication, it is also possible to combine POP before SMTP, APOP, SMTP authentication or encryption using SSL/TLS.

S/MIME ENCRYPTION

To secure email communication from the MFP to certain recipients, the system supports S/MIME (Secure/ Multipurpose Internet Mail Extensions). S/MIME encrypts the email message and content with a security certificate. Opening S/MIME encrypted emails requires the decryption key (private key).

CHANGING "FROM" ADDRESS

When user authentication is activated, it is not possible to change the 'From' address; it will always be the logged-in user's email address. This feature prevents spoofing and provides audit trails for administrators.

FAX REROUTING

Incoming faxes can be automatically forwarded to any destination in the internal address book, including email addresses or the user boxes on the device's internal HDD. Storing incoming faxes in a user box is considerably safer since prints are not left in the output tray. It also speeds up communication as faxes reach recipients sooner. It saves paper – the recipient can decide whether the fax needs to be printed.

FAX LINE SECURITY

Using only the fax protocol for communication no other communication protocols are supported – provides advanced fax line security. Itec devices block any intrusion attempts as threats, including intrusions of a different protocol over public telephone lines, as well as any attempt to transmit data that cannot be decompressed as fax data.

MANUAL DESTINATION PROHIBIT

This function bars the direct input of an email address or scan destination; only registered destinations from the internal system address book or LDAP can be chosen.

NETWORK ACCESS CONTROL

Most Itec devices support the IEEE802.11x standard for network access control to WANs and LANs. The standard secures the network by shutting down any network communication (e.g. DHCP or HTTP) to unauthorised devices, with the exception of authentication requests.