How Safetica helps to comply with ISO/IEC 27002

ISO/IEC 27002 is the information security standard which defines more than **100 recommendations that can help you protect your organization.** These best practices create secure company environment where you minimize risk of business data leaks which cost money, troubles and also customers' trust.

Although compliance with ISO/IEC 27002 includes physical measures (e.g. defining areas with restricted access) most of its **security policies can be met with an appropriate software** and with a change of organizational processes.

Safetica Data Loss Prevention solution will help you protect personal data, register all security incidents and report any relevant events. However, it is not enough to react to security issues. It is important to prevent them. **With Safetica you can do both.** And even more.

What ISO/IEC 27002:2013 requires		How Safetica helps
5 Information security policies		
5.1 Management direction for information security	5.1.1 Policies for information security	Security policies
6 Organization of information security		
6.1 Internal organization	6.1.1 Information security roles and responsibilities	Access management
	6.1.2 Segregation of duties	Access management
6.2 Mobile devices and teleworking	6.2.1 Mobile device policy	Device control
7 Human resource security		
7.2 During employment	7.2.1 Management responsibilities	DLP tools, Supervisor tools
8 Asset management		
8.1 Responsibility for assets	8.1.1 Inventory of assets (partly)	Files monitoring, DLP protocol
	8.1.3 Acceptable use of assets	Security policies in informative mode
8.2 Information classification	8.2.1 Classification of information	File tagging, Data categories
	8.2.2 Labelling of information (partly)	File tagging, Data categories
	8.2.3 Handling of assets	DLP tools, Supervisor tools
8.3 Media handling	8.3.1 Management of removable media	Device control, Security policies
	8.3.3 Physical media transfer	Encryption

What ISO/IEC 27002:2013 requires		How Safetica helps
9 Access control		
9.1 Business requirements of access control	9.1.1 Access control policy	Security policies, Disk Guard
	9.1.2 Access to networks and network services	Web control
9.2 User access management	9.2.2 User access provisioning	Supervisor tools, DLP tools
	9.2.6 Removal or adjustment of access rights	Removal of security keys or passwords database
9.4 System and application access control	9.4.1 Information access restriction	Supervisor tools, DLP tools
	9.4.4 Use of privileged utility programs	Application control
	9.4.5 Access control to program source code	DLP tools
10 Cryptography		
10.1 Cryptographic controls	10.1.2 Key management	Security keys
12 Operations security		
12.1 Operational procedures and responsibilities	12.1.3 Capacity management (partly)	Auditor tools as applications and files monitoring
12.2 Protection from malware	12.2.1 Controls against malware	Antikeylogger, Application control
12.4 Logging and monitoring	12.4.1 Event logging (partly)	Users activity, Clients information
	12.4.2 Protection of log information	Encrypted communication, stored in Database, DLP tools
	12.4.3 Administrator and operator logs	Safetica logs, Access logs
13 Communications security		
13.1 Network security management	13.1.1 Network controls (partly)	DLP tools, Auditor tools
13.2 Information transfer	13.2.1 Information transfer policies and procedures	DLP tools
	13.2.2 Agreements on information transfer	File tagging, Security policies, Encryption
	13.2.3 Electronic messaging (partly)	Encryption, DLP tools
14 System acquisition, development and maintenance		
14.1 Security requirements of information systems	14.1.1 Security requirements analysis and specification	Auditor tools
14.3 Test data	14.3.1 Protection of test data	DLP tools
16 Information security incident management		
16.1 Management of information security incidents and improvements	16.1.2 Reporting information security events	Reports, Alerts
	16.1.7 Collection of evidence	Safetica logs
18 Compliance		
18.1 Compliance with legal and contractual requirements	18.1.2 Intellectual property rights	Regulatory compliance
	18.1.3 Protection of records	DLP tools
	18.1.5 Regulation of cryptographic controls (partly)	Security keys, Encryption