

Ticking off CyberFundamentals Basic: the checklist for an office on Canvos

The CyberFundamentals framework of the Centre for Cybersecurity Belgium is the Belgian yardstick for NIS2 and for any organisation that wants to show the basics are in order. This checklist walks through the measures of the Basic level and shows per measure what Canvos handles by default, what you configure yourself and what falls outside the workplace. With a printable PDF.

Built in = on by default or one setting · Partly = needs your choice or addition · Your policy = outside the workplace

Identify: know what you have

	Status	Date	Owner
☐ Inventory of users and access The user list in organisation management shows every account with role, status, storage and mailbox. Export as CSV for your inventory.	built in		
☐ Inventory of devices Active sessions show device and browser per user. Laptops and phones themselves you keep in your own register.	partly		
☐ Inventory of software and cloud services Canvos replaces mail, files, office suite, chat, meetings and password vault: one supplier on the list instead of six. Other software you keep inventorying yourself.	partly		
☐ Policy and legal requirements An information security policy, GDPR processing register and NIS2 registration at the CCB. See the checklist for the processing register.	your policy		
☐ Supplier risk Canvos runs in Europe with a Belgian provider, without a US parent company; the processing agreement and the location of the data are fixed.	built in		

Protect: access, data, backup, awareness

	Status	Date	Owner
☐ Identities and strong authentication (MFA) Two-factor authentication with authenticator app or hardware key per user; one login for all modules.	built in		
☐ Least privilege and roles Roles & Apps decide who sees which module; company folders give rights per group.	built in		
☐ Remote and mobile access Mobile policy: screen protection, biometric unlock, automatic locking. Sessions can be ended remotely.	built in		
☐ Data protected at rest and in transit TLS everywhere, encrypted backups (AES-256), data classification with labels, DLP on national register numbers and IBANs, sharing policy with password and expiry.	built in		
☐ Backups made, kept and tested Daily encrypted backups with retention are one setting. The yearly restore test you plan and document yourself.	partly		
☐ Secure baseline configuration and patching Servers, updates and security patches are managed by Canvos; executable files and attachments are blocked by default.	built in		
☐ Removing access on departure Disabling one account closes mail, files, calendar, chat and vault at once; sessions expire.	built in		

☐	Awareness and training A yearly session on phishing and passwords remains necessary. The guides on this site can serve as training material.	your policy
☐	Logs kept Login log and governance events, hashed and anchored daily, kept according to the retention policy.	built in

Detect: see what happens

	Status	Date	Owner
☐	Events collected and correlated Every policy action in the evidence chain; export as CEF to a SIEM, or CSV and JSON.	built in	
☐	Suspicious sign-ins New country or new IP is flagged, repeated failed attempts lock temporarily, approval may be required.	built in	
☐	Malicious code Executable files and attachments are blocked and mail is filtered for spam and malware. Endpoint protection on laptops remains your choice.	partly	
☐	Alerts to the right people Real-time alerts and a monthly compliance report to the addresses you set.	built in	

Respond: when things go wrong

	Status	Date	Owner
☐	Incident plan Who calls whom, what is reported to the CCB within 24 and 72 hours. One page suffices for Basic; keep it in the vault.	your policy	
☐	Analysis: what happened Login log plus evidence chain reconstruct in minutes who shared or opened which file.	built in	
☐	Containment End sessions, disable account, reset password, legal hold on affected files.	built in	
☐	Communication and notification The export delivers the facts for the notification; the notifying itself and communication with those affected is yours.	partly	

Recover: back to work

	Status	Date	Owner
☐	Restore from backup Restorable yourself with your own key, without a ticket to a vendor.	built in	
☐	Recovery plan and test Document who restores, where the key is and how long it may take. Test at least yearly.	partly	
☐	Lessons and improvement After an incident: what do we change in policy and settings? The compliance score shows the effect immediately.	your policy	

Working document accompanying the guide on canvos.eu. Not an official assessment.