

Information Security Policy

Seba Agency UG (haftungsbeschränkt) · Version 1.0 · Effective Oct 13, 2026 · Owner: Joshua Omosebi, Managing Director · Review: annually

1. Purpose and scope

This policy sets the minimum security rules for Seba Agency UG (haftungsbeschränkt) (“Seba Agency”, “we”). It applies to everyone who works for or with us and has access to our systems or data (founders, employees, freelancers), to every device used for company work, and to every system we operate, in particular our self-hosted n8n automation server and the integrations running on it, including the TikTok Shop creator and affiliate integration.

2. Roles and responsibilities

- **Managing Director (Joshua Omosebi):** owns this policy, approves access, and acts as security and incident lead.
- **Everyone with access:** follows this policy, completes the security baseline in section 4 before receiving access, and reports suspected incidents immediately under the Incident Response and Breach Notification Policy.
- Everyone with access acknowledges this policy in writing (section 11).

3. Systems in scope

System	Purpose	Hosting location
n8n (self-hosted via Coolify)	Automation workflows, including the TikTok Shop integration	Hetzner Online GmbH
Notion	Database for creator, order and commission records	Notion Labs, Inc., USA
Tally	Forms	Tally BV
TikTok Shop / TikTok APIs	Source of creator, order and commission data	TikTok

System	Purpose	Hosting location
GitHub, Cloudflare	Website code and DNS	USA / global

The complete list of systems and who can access them is kept in the access register of the Access Control Policy.

4. Security baseline for devices and accounts

Every device used for company work must have:

1. Automatic operating system and browser updates switched on.
2. Built-in malware protection active (Microsoft Defender on Windows; XProtect and Gatekeeper on macOS).
3. Full-disk encryption switched on (FileVault on macOS, BitLocker on Windows).
4. Automatic screen lock after at most 5 minutes of inactivity, unlocked by password, PIN or biometrics.
5. No shared user accounts on the device.

Every account used for company work must have:

1. A unique password of at least 12 characters, stored in a password manager.
2. Two-factor authentication (2FA) wherever the service supports it. 2FA is mandatory for email, n8n, Hetzner and Coolify, Notion, Tally, TikTok, GitHub and Cloudflare.
3. Passwords are never sent by chat or email. Where a shared login cannot be avoided, it is shared through the password manager and recorded in the access register.

5. Server and network security

The n8n server is configured and kept as follows:

- **Firewall:** only ports 80 and 443 (HTTPS) and SSH are publicly reachable; all other ports are closed (Hetzner Cloud Firewall and/or ufw).
- **SSH:** key-based login only; password login and direct root login are disabled.
- **Transport encryption:** all web interfaces and webhooks use HTTPS with TLS 1.2 or higher. Plain HTTP redirects to HTTPS.

- **n8n access:** the n8n editor requires a named personal login with 2FA. Webhooks that receive data are authenticated (secret header, token or signature check) wherever the sending platform supports it.
- **Secrets:** API keys and tokens are stored only in n8n's encrypted credential store or in the Coolify environment settings, never in workflow code, Notion or documents. The n8n encryption key is backed up securely and separately from the server.
- **Segregation:** the server runs only Seba Agency services. Each service runs in its own container, and databases are not exposed to the internet.
- **Monitoring:** an uptime monitor alerts on outages; failed n8n executions trigger an alert; server login attempts are logged. Logs are reviewed after every alert and at least monthly.

6. Data protection

Data is classified and handled according to the Data Classification and Handling Policy. The TikTok Shop integration processes only creator usernames and IDs, order IDs, SKU quantities and commission amounts. It must not collect buyer names, addresses, phone numbers or email addresses.

7. Suppliers

We use only suppliers that provide adequate security and, where they process personal data for us, have signed a data processing agreement (Art. 28 GDPR). Current processors are listed in the Internal Data Protection Policy.

8. Backups

The n8n database and configuration must be backed up at least daily, stored encrypted and kept for 30 days. A restore is tested at least once a year.

9. Related policies

Access Control Policy · Data Classification and Handling Policy · Incident Response and Breach Notification Policy · Vulnerability and Patch Management Policy · Internal Data Protection Policy.

10. Exceptions and violations

Exceptions need written approval from the Managing Director, with a reason and an end date. Violations can lead to removal of access and, for contractors, termination of the engagement.

11. Review and acknowledgement

This policy is reviewed at least once a year and after any significant incident or system change.

Name	Role	Signature	Date
Joshua Omosebi	Managing Director	<i>JoshuaOmosebi</i>	October 13, 2026