

PUBLIC – FOR CLIENTS AND SUPPLIERS

Information Security Policy

How Niletech Ltd keeps client data, personal data, source code and live systems confidential, accurate and available.

Version

1.1

Status

Approved

Approved by

Khaled Elmahdi, Director

Effective from

8 October 2026

Next review

October 2027, or sooner after a major change or a serious incident

1 Purpose

Niletech Ltd ("Niletech", "we") designs, builds, connects, hosts and supports software for our clients. Security is part of everything we do.

This policy explains how we keep information safe. That means keeping it **confidential, accurate and available when needed**. It covers:

- client data
- personal data
- source code
- passwords and keys
- business records
- live systems

We match our security measures to the risks of each project. Details for a specific project, such as where it is hosted, how it is backed up, how it is tested and how quickly we respond, are set out in that project's contract, hosting or support agreement, or data processing agreement.

Our detailed day-to-day procedures are kept in our internal IT security policy.

2 Who and what this policy covers

This policy applies to:

- **People:** our directors, staff and any contractors we approve to work on Niletech or client systems.
- **Our tools:** the devices, accounts, software and services we use to run the business and build software.
- **Client systems and data:** client information and systems that we access, build, manage or host.
- **Our suppliers:** the cloud services and other suppliers we use to deliver our work.

If a client contract or the law asks for stronger security, we follow the stronger requirement. If a client runs a system or hosting account that we don't control, we agree in writing who is responsible for what.

3 Who is responsible

Our directors are responsible for information security. That includes managing risks, choosing the right controls, handling incidents and reviewing this policy.

Everyone with access to company or client information must:

- use it only for approved work

- protect their devices, accounts, passwords and confidential material
- report lost devices, phishing emails, suspected weaknesses or security incidents straight away
- follow any extra rules agreed for a client's project
- never share passwords, and never use unapproved services for confidential information

If we work with contractors or other suppliers, we agree confidentiality, access and security terms with them first.

4 Managing risk

When we plan and deliver work, we think about:

- how sensitive the data is
- how exposed the system is to the internet
- who has access to what
- what the system depends on
- what the impact would be if something went wrong

We:

- **identify** the main risks for each client system and for each significant change
- **choose controls** that match how likely and how serious each risk is
- **discuss** any significant remaining risks or trade-offs with the client
- **look again** at risks after major changes, supplier changes or serious incidents

We agree security requirements, and who is responsible for each one, when we scope a project. We review them during the project.

5 How we handle information

We handle information according to how sensitive it is, and according to any contract or legal requirements.

Type	Examples	How we handle it
Public	Website content, approved case studies	Can be shared publicly once approved.
Internal	Procedures, routine business records	Used only for Niletech business.
Confidential	Client documents, private source code, commercial information	Shared only with people who need it, through secure channels.
Restricted	Passwords, private keys, access tokens, special category personal data	Only people who strictly need it, with extra protection.

We never share, move or reuse information outside the agreed scope of a project.

We don't copy live data into development or test systems unless there's a real need and the client agrees how it will be protected. Where we can, we use anonymised or made-up data instead.

6 Accounts and access

We give people **only the access they need** for their work.

- **Own accounts:** everyone has their own account. Accounts are never shared, so every action can be traced to a person.
- **Two-factor login:** multi-factor authentication (MFA) is switched on for every service we use that offers it.
- **Client systems:** for client systems we don't control, we use MFA wherever it's available. Any exception is agreed with the client.
- **Passwords and keys:** we never send passwords or keys in plain text, and never store them in source code.
- **Admin access:** admin rights are only used for tasks that need them. Day-to-day work is done in standard accounts.
- **Reviews:** we review access when someone's role changes, and remove it as soon as it's no longer needed.
- **Unused accounts:** on systems we manage, we remove default accounts, unused access and unnecessary services.

For each client application, we agree user roles, permissions, audit logging and login security based on the application's risk.

7 Devices and working from home

Every device used for Niletech or client work must:

- run a supported operating system and software, with security updates installed automatically
- lock with a password, PIN or fingerprint or face recognition, and have its disk encrypted (FileVault on our Macs)
- have malware protection and a firewall switched on
- be used day to day with a standard account, not an admin account
- have unused software removed

On public or shared networks, take extra care.

Report a lost or possibly compromised device straight away, so we can lock it and remove its access.

8 Building software securely

We think about security at every stage, from planning and design to release and support. Depending on the project, this includes:

- designing secure login, permissions, input checking and error handling
- following established guidance, including the OWASP Top 10
- using maintained frameworks and libraries, and fixing known weaknesses according to risk
- reviewing security-sensitive changes before release
- keeping passwords, keys and settings out of source code
- keeping development, test and live systems separate where we can
- releasing changes to live systems in a controlled way, with a plan to roll back
- logging and monitoring to help us find problems and investigate incidents

The client and we agree on security scanning and independent penetration testing based on the system's risk. This policy doesn't claim any certification or test result, or that a system has no weaknesses.

9 Hosting and encryption

Our project documents name the hosting provider, the data centre region and who is responsible for what.

Where we manage hosting, we:

- keep open services to a minimum and limit admin access
- use supported software and install security updates promptly

- encrypt web traffic and admin connections
- protect stored data, passwords and backups in line with the hosting provider's features and how sensitive the data is
- limit access to live systems and record important security events

Before we go live, we agree with the client where their data will be hosted, for example in the UK or EU. If personal data is transferred outside the UK, we check that there is a lawful way to do it.

10 Backups and continuity

Backup arrangements depend on the system. We agree them in the hosting or support agreement.

Where we're responsible for backups, the agreement sets out:

- what is backed up
- how often, how long backups are kept and where they're stored
- who can access backups and who restores them
- any agreed recovery times
- how and when restores are tested

We plan for continuity from the start. Clients hold their own code, documentation and hosting accounts, so another developer could take over if needed. Any other continuity commitments are set out in the client's agreement. A backup can't guarantee that a service will never be interrupted, or that everything can always be recovered.

11 Finding and fixing weaknesses

We look for and fix security weaknesses in the systems we're responsible for. We prioritise them by risk.

- We assess each reported weakness by how serious it is, how easy it is to exploit and what it could affect.
- We fix weaknesses in line with our support agreements and the risk to the system.
- Where the service design calls for it, we keep and review security logs.
- If we find a serious weakness in a client's system, we tell the client and explain how we'll fix it.

Reporting a vulnerability

If you think you've found a security weakness in a Niletech system, email hello@niletech.co.uk. We will acknowledge your report within **3 working days**. How long it takes to investigate and fix depends on the issue and any agreed support terms. Please don't access, change, download or share anyone else's data.

12 Security incidents

A security incident is anything that may put information or systems at risk. For example:

- someone getting into a system without permission
- information being lost or leaked
- malware
- a compromised service
- a serious threat to a system staying available

When an incident happens, we:

1. **Record it:** what happened, which systems are affected and what evidence we have.
2. **Contain it:** limit the damage, starting with the biggest risks to data, users and services.
3. **Fix the cause:** for example, change passwords, correct settings or fix code.
4. **Recover:** restore services and check they work before returning to normal.
5. **Tell people and learn:** notify those we need to, as required by law and our contracts, and record what we learned.

If an incident affects client information, we tell the client without undue delay.

If we process personal data for a client (as a processor), we tell the client (the controller) about any personal data breach without undue delay, in line with our data processing agreement.

If we're the controller, we decide whether the breach must be reported. Where it must, we report it to the Information Commissioner's Office **within 72 hours** of becoming aware of it.

If a contract sets a shorter deadline for telling the client, we follow the contract.

13 Data protection

Niletech is registered with the UK Information Commissioner's Office (ICO), registration number **C1385586**.

We handle personal data in line with UK data protection law, including the UK GDPR and the Data Protection Act 2018. Depending on the work, we act as a **controller** or a **processor**.

When we process personal data for a client, we sign a written data processing agreement. It covers:

- what we process, why, how and for how long
- the types of personal data and the people it relates to
- the client's instructions, confidentiality and security
- any sub-processors and international transfers
- how we help with people's data rights requests, breaches and other legal duties
- returning or deleting the data at the end of the work

We collect and keep personal data only when we need it for legitimate business or contract purposes. When we no longer need it, we delete it securely.

For personal data collected through our website, see our [privacy policy](https://niletech.co.uk/legal/privacy) (niletech.co.uk/legal/privacy).

14 Suppliers and AI services

We use a small number of trusted infrastructure and software suppliers. When we choose a supplier, we consider:

- what information they'll handle
- how important the service is to us
- their security
- the contract terms

When we use AI services for client work:

- **Before we start:** we agree the purpose, the type of data, the provider and the processing terms before any client information is used.
- **Public tools:** confidential or personal information is never entered into unapproved public AI tools.
- **Training:** client data is never used to train public AI models without the client's explicit, informed permission and a lawful basis.
- **Human checks:** AI output and automated actions are checked in proportion to their impact, including by a person where needed.
- **Limited access:** AI-connected tools only get the access they need for the task.

We assess AI features for data exposure, unintended actions, prompt-injection risks and how reliable the output is.

15 Shared responsibility with clients

Security is shared between us, our clients and their other providers. For each project, we agree who is responsible for:

- running and configuring the client's own accounts and systems
- setting up users and permissions, and using the application safely
- hosting, backups, updates and monitoring
- security testing and fixing weaknesses
- reporting incidents, keeping data and handing over at the end of the contract

Clients remain responsible for anything outside what we've agreed to manage. We record any changes to these responsibilities in writing.

16 Reviews and exceptions

Our directors review this policy at least once a year. They also review it sooner if there are important legal, technical, business or threat changes.

Any exception to this policy must be:

- justified and risk-assessed
- approved by a director
- agreed with the client, if it affects a contract or the client's risk

We fix problems found through incidents, testing or reviews in order of risk.

This policy describes the minimum standard we work to. It doesn't replace the specific commitments in a signed client agreement. It doesn't set a guaranteed service level, and it isn't a certification to an external standard.

17 Cyber Essentials

We are working towards **Cyber Essentials certification**, the UK government-backed scheme for basic cyber security controls. **We have not been certified yet.** Until a certificate is issued, please don't take this as evidence that we are certified or have passed an independent assessment.

We will update this section, and only claim certification, once a valid certificate has been issued.

18 Contact

Company	Niletech Ltd, registered in Scotland
Company number	SC770335
ICO registration	C1385586
Website	www.niletech.co.uk
Email	hello@niletech.co.uk · security reports, supplier checks and general enquiries

NILETECH® is a registered trademark of Niletech Ltd in the United Kingdom and/or other countries.