SECURE FORESTS

Dated: 26 June 2026
Review: June 2027

Secure Forests CIC Ltd Company Policy on Data Protection and GDPR Policy

Secure Forests ICO Reference: ZA
*Certificate Attached
Data Protection Officer: Richard Pyshorn

General Statement - Secure Forests CIC Ltd recognises the legal requirements of the Data Protection Act 2018 and GDPR and is committed to safeguarding personal data.

In particular:

- Personal data will be processed fairly and lawfully and, in particular, will not be processed unless –

  At least one of the conditions set out in Section 2 below is met, and

  In the case of sensitive personal data, at least one of the conditions in Section 3 below is also met.

- Personal data will be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

- Personal data will be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

- Personal data shall be accurate and, where necessary, kept up to date.

- Personal data processed for any purpose(s) will not be kept for longer than is necessary for that purpose or purposes.

- Personal data will be processed in accordance with the rights of data subjects under the Data Protection Act.

- Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data will not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. All in country GDPR policies are to obtain and scrutinised to ensure data compliance.

Conditions for processing personal data

- Unless a relevant exemption applies, at least one of the following conditions must be met whenever we process personal data:
- The individual who the personal data is about has consented to the processing.
- The processing is necessary: in relation to a contract that the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

- The processing is in accordance with the "legitimate interests" condition.

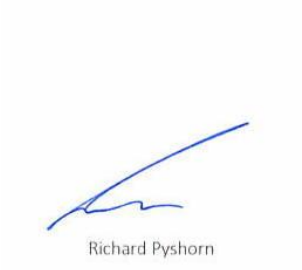
Conditions for the processing sensitive personal data**.**
(As detailed in Schedules 2 to the Data Protection Act 2018).

At least one of the additional conditions listed below must also be met whenever we process sensitive personal data:

- For administering justice, or for exercising statutory or governmental functions the individual who the sensitive personal data is about has given explicit consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of:
  The individual (in a case where the individual's consent cannot be given or reasonably obtained), or another person (in a case where the individual's consent has been unreasonably withheld).
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition. All permissions in writing and on file.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
  The processing is necessary.
- The processing is necessary for medical purposes and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals

In addition to the above conditions which are all set out in the Data Protection Act itself regulations set out several other conditions for processing sensitive personal data. Their effect is to permit the

processing of sensitive personal data for a range of other purposes typically those that are in the substantial public interest, and which must necessarily be carried out without the explicit consent of the individual.
Examples of such purposes include preventing or detecting crime and protecting the public against malpractice or maladministration.
A full list of the additional conditions for processing is set out in the Data Protection (Processing of Sensitive Personal Data) Order 2000 and subsequent orders.



richard@secureforests.com
tellmemore@secureforests.com

Mobile: 0044(0)07854149475
Office:0044(0)1752823601
http://www.secureforests.com/

SECURE FORESTS


General Data Protection Regulation (GDPR)
Everyday Dos and Don'ts
Non-compliance with GDPR can result in fines up to €20 million or 4% of global turnover.
Dos
Shred personal data if in paper form.
Arrange certified confidential waste disposal for large amounts of personal data.
Keep your usernames and passwords secure.
Dispose of personal data promptly.
Report any data breaches immediately.
Undertake regular training on GDPR.
Be vigilant with emails and attachments.
Familiarise yourself with your organisation's documentation and policies.
Log out when not using a digital service.
Only use personal data if you need to, and for as long as you need it.
Audit the data you are using on a day to day basis within the scope of GDPR.
Verify an individual before handing over personal data.
Don'ts
Leave any personal information lying around.
Give your username or password to anyone.
Dispose of personal data in regular bins or recycling if it has not been shredded or destroyed.
Open emails or attachments from unknown sources.
Duplicate personal data unnecessarily e.g. printing it out.
Download business data onto personal devices unless authorised.
Leave your computer logged in if you can access personal data from it.
Store your passwords in browsers.
Log on to public Wi-Fi or unsecured networks whilst working with personal data.
Provide access to personal data unless it is necessary and lawful.
The Data Protection Officer (DPO) or relevant individual in your organisation is:
Intended for unofficial guidance only.
For the complete official legislation and guidance on the General Data Protection Regulation (GDPR) visit ico.org.uk
GDPR MADE SIMPLE
GDPR
SP027A5

SECURE FORESTS

Cyber security policy

OBJECTIVE

The purpose and objective of this Information Security Policy is to protect the company's information assets (note 1) from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

POLICY

- *The Directors Secure Forests CIC Ltd has approved the Information Security Policy.*
- *It is the Policy of the Secure Forests CIC Ltd to ensure that:*

    a. *Information will be protected from a loss of confidentiality (note 2), integrity (note 3) and availability (note 4).*
    b. *Regulatory and legislative requirements will be met (note 5).*
    c. *Business continuity plans will be produced, maintained and tested (note 6).*
    d. *Information security training will be available to all staff.*
    e. *All breaches of information security, actual or suspected, will be reported to, and investigated by, the Information Security Manager.*

- *Guidance and procedures will be produced to support this policy. These may/will include risk assessment, information classification, data protection, credit card handling (PCI), incident handling, information backup, system access, third party services (supplier due diligence), malware controls, mobile device security & remote working, passwords and encryption.*
- *The role and responsibility of the designated Information Security Manager (note 7) is to manage information security and to provide advice and guidance on implementation of the Information Security Policy.*
- *The designated owner of the Information Security Policy Richard Pyshorn] has direct responsibility for maintaining and reviewing the Information Security Policy.*
- *All managers are directly responsible for implementing the Information Security Policy within their business areas.*
- *It is the responsibility of each employee to adhere to the Information Security Policy.*

NOTES

1. *Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation.*
2. *Confidentiality: ensuring that information is accessible only to authorised individuals.*
3. *Integrity: safeguarding the accuracy and completeness of information and processing methods.*
4. *Availability: ensuring that authorised users have access to relevant information when required.*
5. *This includes the requirements of legislation such as the Companies Act, the Data Protection Act, the Computer Misuse Act and the Copyright, Design and Patents Act.*
6. *This will ensure that information and vital services are available to users whenever they need them.*
7. *Depending on the size and nature of the business this may be a part or full-time role for the nominated person.*

Mobile device policy

1. Introduction

Mobile devices, such as smartphones and tablets, are important tools for our organisation. However, mobile devices also represent a significant security risk as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the organisation's data and IT infrastructure. This can subsequently lead to data breaches and system infection.

Secure Forests CIC Ltd has a requirement to protect its information assets to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe and secure use of mobile devices.

2. Roles & Responsibilities

Richard Pyshorn is responsible for maintaining this policy and ensuring that it is fully implemented.

3. Policy Scope

- All mobile devices, whether owned by *Secure Forests CIC Ltd* or owned by employees, that have access to corporate networks, data and systems, not including corporate IT-managed laptops. This includes smartphones and tablet computers.
- Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment must be conducted, and any exemption authorised by *<Manager>.*

1. Policy

1.1 Technical Requirements

1. Devices must use the following Operating Systems: Android or later, IOS or later.

2. Devices must have data encryption enabled at all times.
3. Devices must be configured with a secure PIN/password that complies with Secure Forests password policy. This password must not be the same as any other credentials used within the organisation. In addition, where supported, devices should be secured using biometric security (e.g. Touch ID).
4. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

1.2 User Requirements

1. Users must report all lost or stolen devices to *Secure Forests* IT immediately.
2. If a user suspects that unauthorised access to company data has taken place via a mobile device, they user must report the incident to *Richard Pyshorn*
3. Devices must not be "jailbroken" * or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
4. Users must not load pirated apps/software or illegal content onto their devices.
5. Applications must only be installed from official platform-owner approved app stores. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source contact *Richard Pyshorn*
6. Devices and all apps/software must be kept up to date with manufacturer-provided patches/updates.
7. Users should avoid the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in the body of text or as an attachment, they must notify *Richard Pyshorn* immediately.
8. (If applicable to your organisation) Users must not use corporate workstations to backup or synchronise device content such as media files unless such content is required for legitimate business purposes.

*To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorised software.

Password policy

Why it matters

A robust password policy is essential for all organisations regardless of size.

A password can be extremely valuable to someone with nefarious intentions as it could allow unauthorised access to a business' internal networks. Your most critical data should not rely solely on a password - especially if it accessible from the Internet. Any Internet-facing accounts (for example email, CRM, finance) should be protected by a second factor. This is called two-step (or two-factor) verification. All major platforms support this and it provides much stronger protection against things like phishing or having your password stolen on a malicious Wi-Fi network.

Key takeaways

- • We should use technology to help us use passwords securely. Apps called password managers take the pain out of remembering multiple passwords. You should try to get your users to adopt this. It helps prevent users sharing passwords

between accounts which can lead to serious security breaches if any of those accounts are hacked.

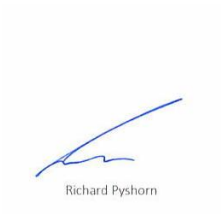
- • If you only have a few users take advantage of the alerting service offered by Troy Hunt who runs https://haveibeenpwned.com/. This website tracks breaches and alerts if email addresses appear in them. You can register your email address(es) with them.

Policy & procedures

- - You should blacklist the most common passwords (such as password123).
- - To make it harder for people to guess what a password is you should ensure that all user passwords contain at least 14 characters and use a selection of letters, numbers and symbols: A-Z, 0-9, @ # $ % ^ & * - _ + = [] { } | \ : ` , . ?/ ` ~" > <( ) ;

Suggest that employees use passphrases rather than passwords. This could be an actual phrase (TheCatSatOnTheMat?184) or a selection of words (1TangoZuluFoxtrot!2). Substituting numbers and symbols for letters and spaces will also help to further strengthen passphrases: S3cur3_Pa55w0rd5_Ar3_Important!

- - If you are using complex password you don't need to change them very often (or at all). Just ask users to change them if they believe the password may have been compromised (such as after a laptop theft).
- - To prevent brute force attempts, implement a temporary internal account lockout feature that activates after five or ten failed attempts. This lockout could be for a set period of time – for example, ten minutes – or require IT support to unlock the account.
- - Where possible, insist that employees activate two-factor authentication on external accounts that are used by your organisation. Using two-factor authentication adds an extra layer of protection to an account and blocks log-in attempts from new or unknown locations even if the password entered is correct.
- - Consider the use of a password manager to help employees create and store strong and complex passwords without the need to remember them. The master password for the manager should be as strong as possible.
- - Make sure that you change the default username and password for any software or equipment (smart TVs, broadband routers etc.) you install.



*Signed_*

Title: Director Secure Forests CIC LTD

Appointed Cyber Security Officer