POLICY DOCUMENT

Information Security Policy

Author:	**Intentional IT Ltd.**
Version Number:	**1**
Version Date:	**July 2024**

Information Security Policy

Contents

Section Title	Page
Introduction	3
Policy Statement	3
Scope of the Policy	3
Equality Impact Assessment	4
Principles	4
Responsibilities	5
Spotless Policy, Procedure, Practice and Guidance	5
Monitoring and Review of Policy	5
Appendix A: Specific Issues and Security Controls	6
Appendix B: Cyber Essentials	

Information Security Policy

Introduction

The purpose of this policy is to protect Spotless Commercial Cleaning from information security problems that might have an adverse effect on its operations, business and reputation.

Spotless Commercial Cleaning relies on the right information being available at the right time, to the right people, in order to satisfy its duties and achieve the outcomes they require. Spotless Commercial Cleaning also has a legal duty to manage personal and personal sensitive information in accordance with the General Data Protection Regulation 2018 and other regulatory and legislative requirements.

Security problems or failure to comply with the Information Security Policy could harm the ability of Spotless Commercial Cleaning to achieve its aims and security objectives, and could damage the professional reputation of the business.

Policy Statement

Spotless Commercial Cleaning is committed to fulfilling its responsibilities with regard to good corporate governance and will act, in good faith, to promote the success of the organisation and demonstrate its commitment to meeting its legal obligations whilst respecting privacy, rights and freedoms under the Data Protection Act, 2018 and related legislation.

Information is vital to Spotless Commercial Cleaning and without it, virtually all operations would cease. The ability to receive, develop, analyse and publish information responsibly enables Spotless Commercial Cleaning to maintain and improve its reputation and ensure that business goals are met.

Information may exist in many forms: it may be printed or written on paper, stored electronically, transmitted by post or using electronic means, or spoken in conversation. Information should always be appropriately protected, whatever form it takes, or means by which it is shared or stored.

Spotless Commercial Cleaning will endeavor to do all it can to protect its information assets in ways that are appropriate and effective.

Scope of the Policy

This policy applies to all Spotless Commercial Cleaning staff, whether permanent or temporary, volunteers, apprentices, contractors and any other person who uses Spotless Commercial Cleaning facilities and information. The policy uses the term “Staff” to encompass all of these groups.

Security problems can include confidentiality (people obtaining or disclosing information inappropriately), integrity (information being altered or erroneously validated, whether deliberate or accidental) and availability (information not being available when it is required).

A wide definition of security will be used to include all types of incident that pose a threat to the effective use of information. This includes performance, consistency, reliability, accuracy and timeliness.

Equality Impact Assessment

In accordance with the Equality Act 2010, Spotless Commercial Cleaning aims to design and implement policies and procedures that meet the diverse needs of our workforce, and seeks to ensure that no person is placed at a disadvantage to any other person.

In accordance with Spotless Commercial Cleaning Equality Impact Assessment (EqIA) policy and procedures, this document has been assessed for its impact upon equality, and reflects the findings of anything identified by the EqIA procedure.

Principles

Spotless Commercial Cleaning will:

- Use all reasonable, appropriate, practical and effective security measures to protect its important processes and assets in order to achieve the security objective.
- Utilise BS7799: Code of Practice for Information Security Management; as a framework for guiding the approach to managing security.
- Continually review security measures so that the ways in which the business is protected improve.
- Protect and manage information assets to meet contractual, legislative, privacy and ethical responsibilities.

Information Assets include (not an exhaustive list):

- Documents (handwritten, typed and annotated copies)
- Reports
- Electronic mail messages
- Diary (e.g. Outlook calendar and desk diaries)
- Computer files (project files, word documents, excel spreadsheets, presentations)
- Intranet and Internet Web pages

Responsibilities

Spotless Commercial Cleaning has a responsibility to make sure that the information assets and infrastructure of Spotless Commercial Cleaning are protected.

All staff and sub-contractors are obliged to comply with this and will, at all times, act in a responsible, professional and security-aware way, maintaining an awareness of and conformance to this Policy. Everyone will respect the information assets of third parties whether or not such protection is required contractually, legally or ethically.

All members of staff and sub-contractors are responsible for identifying security shortfalls in existing security practices and/or improvements that could be made. These should be reported to a Line Manager and then escalated to InTentional IT Ltd.

All staff who have supervisory responsibility are required to actively promote best practice amongst their supervised staff.

The Directors have ultimate responsibility for ensuring that information within Spotless Commercial Cleaning is adequately protected. The responsibility for approving and reviewing access rights to information will be delegated to: Carron Henley, CEO.

Spotless Group Policy, Procedure, Practice and Guidance

The following documents must be read and complied with by all Spotless Commercial Cleaning users of personal information:

- Data Protection Policy and Procedure
- Data Subject Access Procedure
- Privacy Notice
- The Use of Social Media Websites for Business Purposes / Personal Purposes
- Termination of Employment Procedures

Monitoring and Review of Policy

The Information Security Policy will be reviewed and amendments approved, annually, by the Directors.

The Management Team is responsible for ensuring staff understand and comply with the measures that are in place to support the implementation of the Information Security Policy.

Appendix A – Specific Issues and Security Controls

All information (including third party information) will be protected by security controls and handling procedures appropriate to its sensitivity and criticality.

Risk Management

The company will identify security risks and their relative priorities, responding to them promptly and implementing safeguards that are appropriate, effective, culturally acceptable and practical.

Access Control

Access to the Spotless Commercial Cleaning IT systems listed in the information asset register is controlled by the use of User IDs and passwords. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Spotless Commercial Cleaning IT systems. Users will be given access to Spotless Commercial Cleaning systems only to the extent necessary for them to carry out their role, and are expected to work within the limits of their authorisation or specific business need to interrogate a system or data. Authorisation levels will be reviewed on a regular basis.

Individuals must not:

- Allow anyone else to use their user ID or password.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to systems, settings or information.
- Attempt to access data that they are not authorised to use or access.
- Connect any non authorised device to the network or IT systems.
- Store company data on any non-authorised equipment.
- Give or transfer data or software to any person or organisation outside without the authority of the Directors

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

Business Continuity

Spotless Commercial Cleaning have plans to ensure that its activities can continue with minimal disruption, or other adverse impact, should it suffer any form of disruption or security incident. IT systems have been designed to be resilient and available to match the needs of Spotless Commercial Cleaning and are backed up to ensure protection against data loss or corruption.
Spotless Commercial Cleaning backups are stored offsite and the retention periods for backups are determined by the needs of Spotless Commercial Cleaning and consideration of legislative requirements.

Monitoring and filtering
All data that is created and stored on Spotless Commercial Cleaning systems is the property of Spotless Commercial Cleaning and there is no official provision for individual data privacy, however, wherever possible, Spotless Commercial Cleaning will avoid opening personal emails. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

Spotless Commercial Cleaning has the right (under certain conditions) to monitor activity on its systems, including telephones, internet and email use, in order to ensure systems security and effective operation, and to protect against misuse. Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 2018 and the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

Personnel security
All staff and sub-contractors will be responsible for their actions with regard to information security. All Spotless Commercial Cleaning equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Spotless Commercial Cleaning at termination of contract. All data or intellectual property developed or gained during the period of employment remains the property of the business and must not be retained beyond termination or reused for any other purpose. When a user has left the organisation or the account is no longer required, the IT provider should be informed with immediate effect as they will ensure that the user accounts are removed when they are no longer required.

Physical security *Computer/Mobile Device and Data Theft*
If computers, tablets and smartphones are not suitably physically protected, it will make it easier for criminals to not only steal the devices themselves, but to access and/or steal the data contained on them. They will also be open for infection with various kinds of malware– without the criminal needing online access. In spite of the sophisticated online methods now used by criminals, it is still easier to access systems and data by physically doing so on the premises, or taking devices.

If the offices of Spotless Commercial Cleaning, home offices or other sites where computer equipment is kept are not adequately secured, the way is left open for criminals to gain access by breaking in. All staff must ensure their device(s) are locked and hidden out of sight if not in use.

Physical Damage
Like everything else in Spotless Commercial Cleaning, computing and communications devices and infrastructures are vulnerable to damage from fire, flood and accidental damage. Spotless Commercial Cleaning have taken precautions to protect them against such eventualities and have a business continuity plan in place. All Spotless Commercial Cleaning data is backed up offsite.
To avoid physical damage, theft and or access to sensitive records, below are some precautionary steps that can be taken to minimise risk.

Keep devices safe:

- Keep doors and windows locked.
- Keep sensitive hard copy records locked away if possible.
- Make use of an intruder alarm if one is installed.
- Ensure that a fire extinguisher suitable for use with electrical equipment is near the computer.
- Keep food and drink away from computer equipment.
- Ensure that if the device or storage media is no longer required it is returned to your line manager to ascertain if it can be repurposed or securely disposed of.

Visitors to Spotless Commercial Cleaning

Staff must be vigilant about granting access to any visitors, and escort them where appropriate. Restrict access to sensitive areas, such as server rooms. Staff are encouraged to challenge unescorted strangers.

Additional advice for laptop, tablet & smartphone users

All mobile devices and portable storage media should be encrypted.

Staff should keep mobile devices with them at all times. When unattended – for example in a hotel room or meeting room – they should keep them hidden or physically locked away. They should also be carried in hand baggage on an aircraft or coach.

Laptops, tablets and smartphones should never be left on a vehicle seat. Even when the driver is in the vehicle, their device could be vulnerable when stationary (for example, whilst parking or at traffic lights).

Employees with tablets and smartphones should do their best not to have them on display when out and about owing to the increasing trend of snatch robberies, sometimes involving physical violence.

Use padded bags to carry laptops and, where feasible, tablets. Many laptops are broken simply by dropping them.

Hard copy records

Use lockable filing cabinets.

Have a 'clear-desk' policy and lock up sensitive papers when not working on them.

Pick up documents from printers, faxes, photocopiers and multi-functional devices promptly. Where available, use the secure print feature.

Ensure that records that do not need to be retained (in line with the Spotless Commercial Cleaning retention policy) are disposed of securely.

If hard copies must be taken out of Spotless Commercial Cleaning buildings, record their

removal and return, keep them in a secure folder and keep them secure at all times.

Stolen or lost equipment

Staff should notify their manager and then escalate to Intentional IT Ltd at the very earliest opportunity so that they become aware, that any item of Spotless Commercial Cleaning mobile equipment such as phones and laptops, are lost or stolen.

Intentional IT Ltd will ensure that the relevant user account password is changed immediately on receipt of such a theft or loss report.

Staff should notify the Police (or if the theft or loss has occurred on a train, the British Transport Police) and obtain a crime or loss reference number for tracking and insurance purposes.

Internet and Email

Spotless Commercial Cleaning internet and email is intended for business use only. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Spotless Commercial Cleaning in any way, not in breach of any term and condition of employment and does not place the individual or Spotless Commercial Cleaning in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.
Users should not be using the company internet for items such as the below list:

- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Spotless Commercial Cleaning considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Spotless Commercial Cleaning, alter any information about it, or express any opinion about Spotless Commercial Cleaning, unless they are specifically authorised.
- Send unprotected sensitive or confidential information externally.
  Forward Spotless Commercial Cleaning email to personal email accounts.
- Make official commitments through the internet or email on behalf of Spotless Commercial Cleaning unless authorised so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of Intentional IT
- Connect Spotless Commercial Cleaning devices to the internet using non-standard connections.

Telephone Use

All Spotless Commercial Cleaning telephone systems

Staff are permitted to use telephones for personal calls on an occasional basis, and are similarly allowed to receive occasional personal calls. As a guide, "occasional use" in this context means making or receiving no more than one brief personal call per day, although where significant personal issues arise and a member of staff has no other appropriate means of communication available to them, extended use can be accommodated.

Telephone use may be monitored and excessive use of a telephone for personal calls may result in this privilege being withdrawn.

Calls to mobile, fixed tariff and premium rate numbers should be kept to a minimum and less expensive alternatives used where available.

Additional guidance in respect of mobile telephones

For certain roles a mobile telephone is provided and as with all telephones, a mobile phone is to be used for business purposes only.

A mobile phone will remain the property of Spotless Commercial Cleaning and as such all communication via the phone is regarded as business communication. Any personal communication to the phone (verbal or text message) is to Spotless Commercial Cleaning equipment and could be received by persons other than the holder and as a consequence, confidentiality and/or privacy should not be expected.

As with all items of property or equipment, the holder is responsible for the safekeeping of a mobile phone and it should be kept secure at all times. Do not leave a mobile phone in view in an unattended vehicle.

Do not attempt to install a different operating system to the pre-installed operating system on the device.

Remote working

Spotless Commercial Cleaning operates a Virtual Private Network (VPN) and when a remote machine is part of the VPN it effectively creates a new frontier between the Spotless Commercial Cleaning network and the internet. The remote machine now offers a direct route into the Spotless Commercial Cleaning network and all of this policy continues to apply.

If the user is using their own computer, network connection, operating system or software, none of this is controlled by Spotless Commercial Cleaning. The user may be sharing the machine with a number of other users, some of which might not be employed by Spotless Commercial Cleaning. Perhaps the same PC is used to manage corporate documents, as well as material inappropriate for Spotless Commercial Cleaning.

The remote machines must themselves be secured from abuse. Any user accessing the VPN must ensure their own computer has a currently supported operating system, up to date antivirus software, firewall(s) active and all system patches, updates and service packs are installed. If unsure please liaise with Intentional IT in the first instance to minimise risk.

Incident response

Actual or suspected security incidents, including loss of any device containing data or a suspected virus or malware attack, will be reported promptly to the Intentional IT, who will manage the incident. Following recovery from and closure of such incidents, a formal review will take place in order to assess the root cause, identify technical weaknesses or human error, determine the extent of business impact and implement correct action to minimise the risk of similar incidents reoccurring.

Appendix B: Cyber Essentials

The Cyber Essentials framework provides guidance to organisations on the minimum controls that need to be implemented to address the cyber related threats posed and reduce the risk of a breach of the Data Protection Act 1998 and related legislation. This includes controls relating to the five core areas. These core areas and our policy towards them are shown below.

Boundary Firewalls and Internet Gateways

Spotless Commercial Cleaning will:

- install Firewalls or similar devices at the boundaries of the business network
- change all default usernames/passwords on all boundary firewalls (or similar devices) to a strong password
- subject, and document, all open ports and services on each firewall (or similar device) to a justification and approval by an appropriately qualified and authorised business representative
- remove or disable in a timely manner, all firewall rules that are no longer required, and adhere to ongoing monitoring of this
- disable or block by default at the boundary firewalls all commonly attacked and vulnerable services (such as Server Message Block (SMB) NetBIOSm tftp, RPC, rlogin, rsh, rexec)
- disable any remote administrative interface on all firewall (or similar) devices
- where there is no requirement for a system to have Internet access, a Default Deny policy is in effect, applied correctly, preventing the system from making connections to the Internet

Secure Configuration

Spotless Commercial Cleaning will:

- delete or disable all unnecessary or default user accounts
- ensure that all accounts have passwords, and that any default passwords have been changed to strong passwords
- remove or disable all unnecessary software, including OS utilities, services and applications
- disable Auto Run (or similar service) for all media types and network file shares
- install a host based firewall on all desktop PCs or laptops, configured to block unapproved connections by default
- use a standard build image to configure new workstations, including the policies and controls and software required to protect the workstation, and keep this image up to date with corporate policies
- have a backup policy in place, with backups regularly taken to protect against threats such as ransomware
- maintain security and event logs on servers, workstations and laptops

Access Control

Spotless Commercial Cleaning will:

- install malware protection software on all computers capable of connecting outside of our network
- require user account requests to be subject to proper justification, provisioning and an approvals process, and assigned to named individuals
- require users to authenticate with a unique username and strong password before being granted access to computers and applications
- require user accounts to be removed or disabled when no longer required
- restrict to a limited number of authorised users those with elevated or special access privileges, such as system administrator accounts
- document and review quarterly the list of special access privileges
- restrict all administrative accounts to perform administrator activity, with no Internet or external email permissions

Malware Protection

Spotless Commercial Cleaning Ltd will:

- install malware protection software on all computers capable of connecting outside of our network
- require all malware protection software to have all engine updates applied – this must be applied rigorously
- have all malware signature files kept up to date (through automatic updates or through centrally managed deployment
- have malware protection configured for on access scanning, including downloading or opening files, opening folders on removable or remote storage, and web page scanning.
- have malware protection software configured to run regular (at least daily) scans
- prevent users from running executable code or programs from any media to which they also have write access
- prevent users from accessing known malicious web sites by our malware protection software through a blacklisting function

Patch Management

It is Spotless Commercial Cleaning policy to:

- only install licensed and supported software on computers and network devices
- apply software security patches within 14 days of release
- isolate, disable or remove all legacy or unsupported software from devices
- require all mobile devices (including, where authorised, any Bring Your Own Device (BYOD) to be kept up to date with vendor updates and application patches

Date of Review: July 2024
Reviewed by Rhiannon Abbott
HR and Health & Safety Manager