Ideal Cleaning Services Limited

Information Security Policy

This policy document encompasses all aspects of security surrounding confidential Company information and must be distributed to all Company employees that have access to sensitive/confidential information. All such Company employees must read this document in its entirety and sign the form confirming they have read and understand this policy fully. This document will be reviewed and updated by management on an annual basis or when relevant to include newly developed security standards into the policy.

Ethics and Acceptable Use Policies

All company employees are required to conduct business in accordance with all applicable laws, regulations and contractual obligations. All employees must behave ethically, with integrity and adhere to all Company policies and procedures. It is the responsibility of the employee to be truthful, honest and comply fully with information security standards and regulations set out by the Company. In addition to this, an employee must report any inappropriate activity or unlawful conduct by another employee to a senior officer of the Company, whenever and wherever they become aware of the activity.

Consumer confidence is of paramount importance to our business. With this in mind, the security and protection of sensitive information for both personal client information, (i.e. name, address, phone number, email, Social Security number, driver's license number, bank account and credit card numbers, etc.) and Company information that is not readily available to the public (i.e. – client's financial information, employee information, schedules, technology, etc.) is crucial. It is imperative that employees understand the importance of safeguarding such sensitive information from third parties that do not need it to go about their daily business.

Disciplinary Action

Violation of the standards, policies and procedures presented in this document by an employee will result in disciplinary action, from warnings or reprimands up to and including termination of employment. Claims of ignorance, good intentions or using poor judgment will not be used as excuses for noncompliance.

Protect Stored Data

All sensitive cardholder data stored and handled by the Company and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the Company for business reasons must be destroyed in a secure and irrecoverable manner.

Credit Card Information Handling Specifics:

- All media (i.e. paper, backup tape, computer hard drive, etc.) that contains cardholder information must be destroyed securely and irreversibly (i.e. shredding, degaussing, disassembly, etc.) when it is no longer needed.
- It is strictly prohibited to store:
  The contents of the credit card magnetic strip (track data) on any media whatsoever.
  The CVV/CVC (the 3- or 4-digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
  All digits of the credit card primary account number on any media whatsoever.
  All digits but the last four numbers of the credit card account number must be concealed or masked (i.e. x's or *'s) when the number needs to be displayed.

Protect Data in Transit

All sensitive cardholder data must be protected securely if it is to be transported physically or electronically.

Credit Card Information Handling Specifics:

- Credit Card details (PAN, track data etc) must never be sent over the internet via email, instant chat or any other end user technologies without using a strong encryption mechanism (i.e. AES encryption).
- The transportation of media containing sensitive card data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

Restrict Access to Data

Access to sensitive cardholder information such as PANs, personal information and business data is restricted to employees that have a legitimate need to view such information. No other employees should have access to this confidential data unless they have a genuine business need.

Physical Security

Access to sensitive information in both hard and soft format must be physically restricted to prevent unauthorised individuals from obtaining sensitive data. Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive, etc.

- Media containing sensitive cardholder information must be handled and distributed in a secure manner by trusted individuals.
- Media storing sensitive cardholder data (especially the PAN and other personal information such as social security numbers) should be properly logged and inventoried before being destroyed. Sensitive data should always be destroyed when it is no longer required by the company in such a manner as to render the content irrecoverable.
- Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information.
- All computers that store sensitive cardholder data must have a password protected screensaver enabled to prevent unauthorised use.

Security Awareness and Procedures

The policies and procedures outlined below must be incorporated into Company practice to maintain a high level of security awareness. The protection of sensitive data demands regular training of all employees and contractors that have access to sensitive/confidential information.

- Review handling procedures for sensitive information and hold periodic security awareness meetings to incorporate these procedures into day-to-day company practice.
- Distribute this security policy document to all such Company employees to read. It is required that all such employees confirm that they understand the content of this security policy document by signing an acknowledgement form (see Appendix A)

- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).
- Company security policies must be reviewed annually and updated as needed.

Security Management / Incident Response Plan

Employees of the Company will be expected to report to a Director or General Manager of the Company any security related issues. They will effectively communicate all security policies and procedures to employees within the Company and contractors. In addition to this, they will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implementation of the incident response plan in the event of a sensitive data compromise.

Incident Response Plan

- In the event of a suspected security breach, alert a Director or the General Manager immediately.
- They will carry out an initial investigation of the suspected security breach.
- Upon confirmation that a security breach has occurred, they will begin informing all relevant parties that may be affected by the compromise.

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank, Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.

For and on behalf of Ideal Cleaning Services Limited

CHRISTOPHER DRING
Group Managing Director

Reviewed 09-2023

Appendix A – Agreement to Comply Form

Agreement to Comply with Information Security Policies

_____

Employee Name (printed)

_____

Department

I agree to take all reasonable precautions to assure that Company internal information, or information that has been entrusted to the Company by third parties such as customers, will not be disclosed to unauthorised persons. At the end of my employment or contract with the Company, I agree to return all information to which I have had access as a result of my position. I understand that I am not authorised to use sensitive information for my own purposes, nor am I at liberty to provide this information to third parties without the express written consent of the internal manager who is the designated information owner.

I have access to a copy of the Information Security Policies, I have read and understand these policies, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the policies and other requirements found in the Company security policy. I understand that non-compliance will be cause for disciplinary action up to and including dismissal, and perhaps criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of information security policies to the designated management of the Company.

_____

Employee Signature

_____

Date

Reviewed 09-2023