Information Management Guide

Table of Contents

Preface

The information handled by Sublime Streamline Ltd is covered by a series of internal procedures and regulations.

Looking beyond tools and processes, however, every Sublime Streamline Ltd employee needs, first and foremost, to behave in a responsible manner when handling information. Information processing and management are the heart of the Companies business and are key to its performance.

The aim of this Best Practice Guide is to provide a reminder of a few simple rules, and above all to encourage reflection on the ethical and compliance issues associated with responsible information management.

Information management is of vital strategic importance to Sublime Streamline Ltd. In a world that is increasingly mobile, interconnected and interdependent our ability to manage information effectively and securely ensures that clients both existing and potential trust us to look after their data as if it was our own.

In their day-to-day activities, all Sublime Streamline Ltd employees are continuously required to process and manage information, both electronically and physically (in the form of paper documents, and electronic data accessed by Sublime Streamline Ltd SAAS products or via remote access to customer systems). The confidentiality and security of that data is dependent on our systems and people.

The aim of this guide is to help employees manage information in accordance with the legal and ethical requirements with which Sublime Streamline Ltd complies. It does not aim to set out rules of conduct to be followed in all circumstances, but is intended for use by everybody who has to handle information in their work.

.

Employees knowledge of information is often limited to their immediate work environment and or the areas specifically covered by their activities.

The intrinsic value of such partial information held by an employee grows as that information is transmitted and exchanged. Information, when it is shared, supports the decision-making process. Information that appears to be trivial may in fact turn out to be sensitive or otherwise important when utilised in a different context, or when combined with other data.

In all cases, responsibility for protection and disclosure, whether internal or external, rests with

the individual holding the information.

Particular vigilance is required regarding information disclosed on social networking websites. Although such information may appear to be completely separate from the work environment, it can potentially be damaging to the Sublime Streamline Ltd, our customers, employees, their friends or family.

Employees are requested not to disclose information related to Sublime Streamline Ltd customer activities on social networking websites.

If in doubt, ask your line manager for advice, or, depending on the nature of the information, contact the management team at head office.

Acquiring Information

The acquisition of information is an intrinsic part of Sublime Streamline Ltd business activities on behalf of our customers. It is vital that it takes place in accordance with the legal and ethical requirements with which the company complies.

Information can be obtained through legal channels such as client assignment processing, note-taking, brochures, meetings, conferences, websites, free or subscription databases, etc.

Business intelligence

Business intelligence involves gathering, analysing, disseminating and protecting strategic information to support planning and decision-making.

Within Sublime Streamline Ltd, it plays a key role in improving our understanding of markets and customer expectations, as well as providing in-depth information on our competitors and the economic challenges facing the company.

However, Sublime Streamline ltd adopts a zero-tolerance stance on any attempt to acquire information fraudulently by theft or hacking. Sublime Streamline Ltd is liable for such actions. They are subject to strict sanctions in the companies countries of operation. Moreover, they seriously harm Sublime Streamline Ltd image.

Computer hackers violate software, computer or network security systems for malicious purposes, such as theft of confidential information. In addition to being strictly against the law in Sublime Streamline Ltd countries of operation, computer hacking is completely at odds with the companies ethical principles. Sublime Streamline ltd adopts a policy of zero tolerance on any attempt to acquire information by such means.

If information is acquired by chance (for example if an employee finds a RFP pack left on a train or plane, overhears an informal conversation between competitors, or receives documents by mistake), the following actions should be taken.

- Do not make use of the information.
- If possible, and where applicable, return it to its owner.
- If this is not possible, destroy it.
- Report the incident to your line manager and Security officer.

if in doubt, ask your line manager for advice, or, depending on the nature of the information, contact the management team at head office.

Legal Framework

New Zealand

In New Zealand, protection of information is based on several pieces legislation contained in sections of the Crimes Amendment Act 2003 Specific legislation is found for the following offences

Section 229 - **Criminal breach of trust**
Every one is guilty of a criminal breach of trust who, as a trustee of any trust, dishonestly and contrary to the terms of that trust, converts anything to any use not authorised by the trust - .Penalty Imprisonment up to 7 years

Section 230 - **Taking, obtaining, or copying trade secrets**
Anyone who with intent to obtain any pecuniary advantage or to cause loss to any other person, dishonestly and without claim of right, takes, obtains, or copies (or copy) any document or any model or other depiction of any thing or process containing or embodying any trade secret, knowing that it contains or embodies a trade secret. For the purposes of this section, trade secret means any information that is, or has the potential to be, used industrially or commercially and is not generally available in industrial or commercial use and has economic value or potential economic value to the possessor of the information and
is the subject of all reasonable efforts to preserve its secrecy. - Penalty up to 5 years

Section 249 - **Accessing computer system for dishonest purpose**
Anyone who directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right, obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration or causes loss to any other person. - Penalty up to 5 years

Section 250 - **Damaging or interfering with computer system**
Anyone who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result. - Penalty up to 10 years
Anyone who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised, damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system or causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired or causes any computer system to fail or deny service to any authorised users. - Penalty Up to 5 years

Section 252 - **Accessing computer system without authorisation**
Anyone who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system. Penalty up to 2 years

A copy of the NZ Crimes Amendment Act (2003) can be found here -
http://www.legislation.govt.nz/act/public/2003/0039/latest/DLM200200

Australia

In Australia, protection of information is covered by legislation contained in the Cybercrime Act 2001. A person is guilty of an offence if, They commit or cause, any unauthorised access to data held in a computer or any unauthorised access to or modification of data held in a computer, or any unauthorised impairment of electronic communication to or from a computer, and the unauthorised access, modification or impairment and the person knows the access, modification or impairment is unauthorised or the person produces, supplies or obtains data and the person does so with the intention that the data be used, by the person or another person, in and the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment. Penalty range 2 - 10 years dependent offence committed.

A copy of the Australian Cybercrime Act (2001) can be found here
https://www.legislation.gov.au/Details/C2004C01213

Fij

Fiji Information offences are covered by the Crimes Decree 2009 - Division 6 sections 336 to 346 relates to computer offences where a person commits or causes to be allowed unauthorised access, modification or impairment to data held in a computer or data storage device whether or not the conduct or result of the conduct constituting the offence occurs in Fiji. Penalty range 2-10 years

A copy of the Fiji Crimes Decree (2009) can be found here
http://www.fiji.gov.fj/getattachment/604e31fc-c7b1-41a0-9686-71377917b6eb/Decree-No-44---Crimes-Decree-2009-(pdf).aspx

Best Practices

A non-exhaustive list of best practices in information processing is given below, the intention being to help employees manage information at a day-to-day level.

use of information technology

When processing and handling information, employees must use IT resources (hardware, software, information systems and applications) provided and or approved by Sublime Group, and qualified for the level of sensitivity of the information concerned.

In addition, employees are advised to make responsible use of the communications systems and equipment made available to them. Using computers (especially laptops) or smartphones, particularly outside the company, can lead to a risk of leakage of confidential information.

Being vigilant

Files, documents or information whose disclosure and or loss would cause serious harm to Sublime Group should never be left unattended in any circumstances.

This applies in particular when travelling outside the Company, and to visits by third parties to Sublime Group premises.

Conservation of documents

Sublime Group is required to comply with legal procedures and deadlines regarding the conservation and destruction of documents.

These obligations vary from country to country, and are applicable to physical documents as well as information in digital format.

Data Protection Statement

Sublime Streamline Ltd aims to comply with international best practice in data protection and respects your choices in respect of your personal data.

The main purposes for which your personal data is collected, used or disclosed by Sublime Streamline Ltd and its related companies and our re-sellers include providing you with our products and services, managing your subscriptions, renewals and your account, processing payments, addressing questions and feedback, improving our products and services, as well as where permitted under law, sending you marketing and promotional offers on products and services, and personalised content and advertising based on your preferences or demographics.

Sublime Streamline Ltd has a data protection policy which provides more information about how we collect, use and disclose your personal data. Should you have any feedback or enquiries relating to your personal data or if you wish to stop receiving promotional or marketing messages from Sublime Group limited please contact us via our helpdesk helpdesk@sublimegroup.net

For more information please refer to

- Sublime Streamline Ltd Privacy Policy
- Sublime Streamline Ltd Information Management Guide
- Sublime Streamline Ltd Terms and Conditions

Information Security Policy

Security Policy Outline

Overview

This document summarizes the Sublime Streamline Limited comprehensive written Information Security Policy mandated by the PCI DSS Security Compliance Program. In particular, this document describes the Security Policy elements pursuant to which the company intends to (i) ensure the security and confidentiality of card holder data, (ii) protect against any anticipated threats or hazards to the security of such data, and (iii) protect against the unauthorized access or use of such card holder data records or information in ways that could result in substantial harm or inconvenience to customers. The Security Policy incorporates by reference the companies policies and procedures enumerated below and are in addition to any company policies and procedures that may be required pursuant to government laws and regulations.

Revisions to this document are maintained collectively in Appendix A- Revisions, which includes a revision table describing each addition, change or deletion and the date it was implemented. All revisions are referenced using this procedure. The original document will remain intact.

Designation of Representatives

Damian Kobylinksi is designated as the Security Officer who shall be responsible for coordinating and overseeing the Security Policy. The Security Officer may designate other representatives of the company to oversee and coordinate particular elements of the Security Policy. Any questions regarding the implementation of the Security Policy or the interpretation of this document should be directed to the Security Officer or his or her designees.

Scope of Security Policy

The Security Policy applies to all types of sensitive information including any record containing sensitive and confidential information about a employee or a customer who has a relationship with the company, whether in paper, electronic or other form that is handled or maintained by or on behalf of the company or its affiliates. In addition, the Security Officer will work with the legal department to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards to comply with the Company Information Security Policy.

Please see the definition for Information Technology Resources in the next section of this document.

Important Note

For these purposes, the term card holder information includes any information
(i) Provided by the card holder in conjunction with a transaction to purchase or obtain a product or service from the company,
(ii) Elements of the card holder data includes cardholder name, primary account number (PAN), Service Code, Expiration date
(iii) Sensitive Authentication data such as Full Magnetic Stripe, CVC2/CVW2/CID, PIN/PIN Block.

Elements of the Security Policy

Risk Identification and Assessment.

The company intends, as part of the Security Policy, to undertake on an annual basis to identify and assess external and internal risks to the security, confidentiality, and integrity of information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the Security Policy, the Security Officer will establish procedures for identifying and assessing such risks in each relevant area of the companies operations, including:

- Employee training and management. The Security Officer will coordinate with representatives in the Companies other departments or areas to evaluate the effectiveness of the Companies procedures and practices relating to access to and use of card holder data. This evaluation will include assessing the effectiveness of the Companies current policies and procedures in this area.

- Information Systems and Information Processing and Disposal. The Security Officer will coordinate with representatives of the Companies I.T to assess the risks associated with the Companies information systems, including network and software design, information processing, and the storage, transmission and disposal of card holder data and information. This evaluation will include assessing the Companies current polices and procedures relating to [Acceptable Use of the Companies network and network security, document retention and destruction]. The Security Officer will also coordinate with the Companies I.T to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems by, among other things, implementing patches or other software fixes designed to deal with known security flaws.

- Detecting, Preventing and Responding to Attacks. The Security Officer will coordinate with the Companies I.T to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Security Officer may elect to delegate to a representative of the I.T the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the Company.

Designing and Implementing Safeguards.

The risk assessment and analysis described above shall apply to all methods of handling or disposing of sensitive information such as card holder data, whether in electronic, paper or other form. The Security Officer will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

Overseeing Service Providers.

The Security Officer shall coordinate with those responsible for the third party service procurement activities among the I.T and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for protecting card holder data and other third parties to which they will have access. In addition, the Security Officer will work with the legal department to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards to comply with the PCI DSS requirements. Any deviation from these standard provisions will require the approval of the legal department. These standards shall apply to all existing and future contracts entered into with such third party service providers.

Incident Management Policy.

The Companies Information Technology Resources must be protected against events that may jeopardize information security by contaminating, damaging, or destroying information resources. All information security incidents must be reported in accordance with the policies and procedures provided below regardless of whether or not damage appears to have been incurred. The incident management process is the responsibility of the incident Management Manager - Craig Pellett

Adjustments to Security Policy.

The Security Officer is responsible for evaluating and adjusting the Security Policy based on the risk identification and assessment activities undertaken pursuant to the Security Policy, as well as any material changes to the companies operations or other circumstances that may have a material impact on the Security Policy.

Terminology

Security Officer

A person responsible within the company for coordinating and overseeing this Security Policy. The Security Officer may designate other representatives of the Company to oversee and coordinate particular elements of the Security Policy.

Information Technology Resources (ITR)

Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Backup

Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

Offsite Storage

Based on data criticality, offsite storage should be in a geographically different location from the Company campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location on the Company premises may be appropriate.

Vendor

A third party who provides one or more services that includes software, hardware, or other type of service to the company.

Connected Entity

Any foreign entity that is connected to the cardholder environment. In most instances a connected entity will be a connected third party, but this will vary depending on how the company has segmented their environment. In most cases the reference is to third-parties such as VPN connections to acquirers/processors, network connection to vendor or client, external dedicated network connections (i.e. VPN, frame-relay, etc.)

Internet Use Policy

Introduction

This policy is established to achieve the following

- To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of the internet.
- To educate employees, contractors and third parties who may use the internet, the intranet, or both with respect to their responsibilities associated with such use.

Audience

The Internet Use Policy applies equally to all employees, contractors and third parties granted access to any Information Resource with the capacity to access the internet, the intranet, or both.

Ownership

Electronic files created, sent, received, or stored on computers owned, leased administered or otherwise under the custody and control of company are the property of the company.

Privacy

Electronic files created, sent, received, or stored on information technology resources owned, leased, administered, or otherwise under the custody and control of company are not private and may be accessed by company IT employees at any time without knowledge of the Information technology resources user or owner.

Internet Use Policy

- Software for browsing the Internet is provided to authorized users for business use only.
- All software used to access the Internet must be part of the company standard software suite or approved by the Security Officer. This software must incorporate all vendor provided security patches.
- All files downloaded from the Internet must be scanned for viruses using the approved IT distributed software suite and current virus detection software.
- All software used to access the Internet shall be configured to use the firewall http proxy.
- All sites accessed must comply with the company Acceptable Use Policies.
- All user activity on company Information technology resources assets is subject to logging and review.
- Content on all company web sites must comply with the Company Acceptable Use Policies.
- No offensive or harassing material may be made available via company web sites.
- Non-business related purchases made over the internet are prohibited. Business related purchases are subject to company procurement rules.
- No personal commercial advertising may be made available via company web sites.
- Company internet access may not be used for personal gain or non-company personal solicitations.
- No company data will be made available via company web sites without ensuring that the material is available to only authorized individuals or groups.
- All sensitive company material transmitted over external network must be encrypted.
- Electronic files are subject to the same records retention rules that apply to other documents and must be retained in accordance with departmental records retention schedules.

Permitted Use

- Incidental personal use of Internet access is restricted to company approved users - it does not extend to family members or other acquaintances.

- Incidental use must not result in direct costs to company.
- Incidental use must not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal liability for, or embarrassment to, company.
- Storage of personal files and documents within companies information technology resources should be nominal.
- All files and documents including personal files and documents are owned by company, may be subject to open records requests, and may be accessed in accordance with this policy.

Disciplinary Actions for Violation

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of company information technology resources access privileges, civil, and criminal prosecution.

Email Policy

Introduction

This policy is established to achieve the following-

- To ensure compliance with applicable statutes, regulations, and contractual mandates regarding the management of information resources.
- To establish prudent and acceptable practices regarding the use of email.
- To educate individuals using email with respect to their responsibilities associated with such use.

Purpose

The purpose of the Company Email Policy is to establish the rules for the use of Company email for the sending, receiving, or storing of electronic mail.

Audience

The company email policy applies equally to all individuals granted access privileges to any Company information resource with the capacity to send, receive, or store electronic mail

Email Policy

The following activities are prohibited by policy –

- Sending email with any type sensitive information such as credit card data or personally identifiable information (PII).
- Sending email that is intimidating or harassing.
- Using email for conducting personal business.
- Using email for purposes of political lobbying or campaigning.
- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending email, except when authorized to send messages for another when serving in an administrative support role.
- The use of unauthorised e-mail software.

The following activities are prohibited because they impede the functioning of network communications and the efficient operations of electronic mail systems:

- Sending or forwarding chain letters.
- Sending unsolicited messages to large groups except as required to conduct agency business.
- Sending excessively large messages.
- Sending or forwarding email that is likely to contain computer viruses.

All user activity on company information technology resources assets is subject to logging and review.

Electronic mail users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of company or any unit of the company unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing the company. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

Individuals must not send, forward or receive confidential or sensitive company information through email accounts.

Individuals must not send, forward, receive or store confidential or sensitive Company information utilizing non-Company accredited mobile devices. Examples of mobile devices

include, but are not limited to, Personal Data Assistants, Smart phones, Tablets, Blackberry's and cellular telephones.

Disciplinary Actions for Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of Company Information Technology Resources access privileges, civil, and criminal prosecution.

Account Management Security Policy

Introduction

Computer accounts are the means used to grant access to information resources. These accounts provide a means of providing accountability, a key to any computer security program, for information resources usage. This means that creating, controlling, and monitoring all computer accounts is extremely important to an overall security program.

Purpose

The purpose of the Account Management Security Policy is to establish the rules for the creation, monitoring, control and removal of user accounts.

Audience

The Account Management Security Policy applies to all individuals within the company enterprise that are responsible for the installation and support of information resources, individuals charged with information technology resources security, and data owners.

Account Management Security Policy

- All accounts created must have an associated request and approval that is appropriate for the system or service.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with the company password policy.
- All accounts must have a password expiration that complies with the company password policy.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- System administrators or other designated staff are responsible for removing the accounts of individuals that change roles within company or are separated from their relationship with company.
- System administrators or other designated staff are responsible must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes.
- System administrators or other designated staff must have a documented process for periodically reviewing existing accounts for validity.
- System administrators or other designated staff are subject to independent audit review.
- System administrators or other designated staff must provide a list of accounts for the systems they administer when requested by authorized management.

Disciplinary Actions for Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of company information technology resources access privileges, civil, and criminal prosecution.

Physical Access Policy

Introduction

Technical support staff, security administrators, system administrators, and others may have Information Resource physical facility access requirements as part of their function. The granting, controlling, and monitoring of the physical access to information technology resources facilities is extremely important to an overall security program.

Purpose

The purpose of the Company Physical Access Policy is to establish the rules for the granting, control, monitoring, and removal of physical access to Information Resource facilities.

Audience

The company Physical Access Policy applies to all individuals within the company enterprise that are responsible for the installation and support of Information Resources, individuals charged with information technology resources security, and data owners.

Physical Access Policy

- All physical security systems must comply with applicable all applicable regulations such as, but not limited to, building codes and fire prevention codes.
- Physical access to all information technology resources restricted facilities must be documented and managed.
- All ITR facilities must be physically protected in proportion to the criticality or importance of their function at company.
- Access to information technology resources facilities must be granted only to company support personnel, and contractors, whose job responsibilities require access to that facility.
- The process for granting card and/or key access to information technology resources facilities must include the approval of the person responsible for the facility.
- Each individual that is granted access rights to an information technology resources facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements.
- Requests for access must come from the applicable company data/system owner.
- Access cards and/or keys must not be shared or loaned to others.
- Access cards and/or keys that are no longer required must be returned to the person responsible for the information technology resources facility. Cards must not be reallocated to another individual bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the person responsible for the Information technology resources facility.
- Cards and/or keys must not have identifying information other than a return mail address.
- All Information technology resources facilities that allow access to visitors will track visitor access with a sign in/out log.
- A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
- Card access records and visitor logs for information technology resources facilities must be kept for routine review based upon the criticality of the information technology resources being protected.
- The person responsible for the information technology resources facility must remove the card and/or key access rights of individuals that change roles within company or are separated from their relationship with company.
- Visitors must be escorted in card access controlled areas of information technology resources facilities.
- The person responsible for the information technology resources facility must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- The person responsible for the information technology resources facility must review

card and/or key access rights for the facility on a periodic basis and remove access for individuals that no longer require access.

- Signage for restricted access rooms and locations must be practical, yet minimal discernible evidence of the importance of the location should be displayed.

Disciplinary Actions for Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of company information technology resources access privileges, civil, and criminal prosecution.

Incident Management Policy

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

This section describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: virus, worm, and Trojan horse detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Technology Resources as outlined in the Email Policy, the Internet Policy, and the Acceptable Use Policy.

Audience

The company Incident Management Policy applies equally to all individuals that use any company information resources.

Incident Management Practice Standard

- Company Incident Management Team (CIMT) members have pre-defined roles and responsibilities which can take priority over normal duties.
- Whenever a security incident, such as a virus, worm, hoax email, discovery of hacking tools, altered data, etc. is suspected or confirmed, the appropriate incident management procedures must be followed.
- The Security Officer is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation.
- The appropriate technical resources from the CIMT are responsible for monitoring that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
- The Security Officer, working with the Incident Management Manager (IMM), will determine if a widespread company communication is required, the content of the communication, and how best to distribute the communication.
- The appropriate technical resources from the CIMT are responsible for communicating new issues or vulnerabilities to the system vendor and working with the vendor to eliminate or mitigate the vulnerability.
- The Security Officer is responsible for initiating, completing, and documenting the incident investigation with assistance from the CIMT.
- The company Security Officer is responsible for reporting the incident to the Incident Management Manager or government officials as required by applicable statutes and/or regulations
- The Security Officer is responsible for coordinating communications with outside organisations and law enforcement.
- In the case where law enforcement is not involved, the Security Officer will recommend disciplinary actions, if appropriate, to the IMM.
- In the case where law enforcement is involved, the Security Officer will act as the liaison between law enforcement and company.

Disciplinary Actions for Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of company information technology resources access privileges, civil, and criminal prosecution.

Network Access Policy

Introduction

The company network infrastructure is provided as a central utility for all users of company Information Resources. It is important that the infrastructure, which includes cabling and the associated active equipment', continues to develop with sufficient flexibility to meet company demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

Purpose

The purpose of the Company Network Access Policy is to establish the rules for the access and use of the network infrastructure. These rules are necessary to preserve the integrity, availability and confidentiality of Company information.

Audience

The Company Network Access Policy applies equally to all individuals with access to any company information resource.

Network Access Policy

- Users are permitted to use only those network addresses issued to them by companies information technology team.
- All remote access (dial in services) to company will be either through an approved modem pool or via an Internet Service Provider (ISP).
- Remote users may connect to company information technology resources only through an ISP and using protocols approved by company.
- Users inside the company firewall may not be connected to the company network at the same time a modem is being used to connect to an external network.
- Users must not extend or re-transmit network services in any way. This means you must not install a router, switch, hub, or wireless access point to the company network without company IT approval.
- Users must not install network hardware or software that provides network services without company IT approval.
- Non company computer systems that require network connectivity must conform to company IT Standards.
- Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, company users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the company network infrastructure.
- Users are not permitted to alter network hardware in any way.

Disciplinary Actions for Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of company information technology resources access privileges, civil, and criminal prosecution.

Backup & Disaster Recovery Policy

Introduction

Electronic backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, or system operations errors.

Purpose

The purpose of the Company Backup/DRP Policy is to establish the rules for the backup and storage of electronic Company information.

Audience

The Company Backup/DRP Policy applies to all individuals within the Company enterprise that are responsible for the installation and support of Information Resources, individuals charged with Information Resources Security and data owners.

Backup - Disaster Recovery Policy

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- The company information resources backup and recovery process for each system must be documented and periodically reviewed.
- The vendor(s) providing offsite backup storage for company must be cleared to handle the highest level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally backup media must be protected in accordance with the highest company sensitivity level of information stored.
- A process must be implemented to verify the success of the company electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable.
- Signature cards held by the offsite backup storage vendor(s) for access to company backup media must be reviewed annually or when an authorized individual leaves company.
- Procedures between company and the offsite backup storage vendor(s) must be reviewed at least annually. (Please refer to Managing Third Party Vendors Policy for more details)
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
    - System name
    - Creation Date
    - Sensitivity Classification
    - Company Contact Information

Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of company information resources access privileges, civil, and criminal prosecution.

Employee Screening Policy

Introduction

Hiring employees with integrity is important to the company. Screening of employees allows verifying the credentials provided by them. This policy also ensures the company complies with various government and contractual mandates.

Purpose

The purpose of the Policy is to establish the rules for the screening of the employee during their hiring process.

Audience

The company Employee Screening Policy applies to all individuals within the company enterprise who is considering employment with the company.

Employee Screening Policy

- All applicants for employment with company are asked to sign a release form authorizing the appropriate background checks. Any applicant who refuses to sign a release form is no longer considered eligible for employment.
- Applicants also are expected to provide references from their former employers as well as educational reference information that can be used to verify academic accomplishments and records. The background check will include verification of information provided on the completed application for employment, the applicant's resume or on other forms used in the hiring process.
- Information to be verified includes, but is not limited to, social security number and previous addresses. Company will also conduct a reference check and verification of the applicant's education and employment background as stated on the employment application or other documents listed above. The background check may also include criminal court record searches. If a conviction is discovered, a determination will be made whether the conviction is related to the position for which the individual is applying or presents safety or security risks before an employment decision is made.
- Additional checks such as a driving record or credit record may be made on applicants for particular job categories if appropriate and job related. If an applicant is denied employment in whole or in part because of information obtained in his/her background check, the applicant will be informed of this and given the name, address and phone number of the screening provider to contact if s/he has specific questions about the result of the check or wants to dispute its accuracy.

Disciplinary Actions for Violations

Any applicant who provides misleading, erroneous or wilfully deceptive information to the company on an employment form or resume or in a selection interview is immediately eliminated from further consideration for employment with Company.

Awareness and Training

Introduction

Effective information security requires a high level of participation from all employees of the company. Ensuring all individuals understand the security needs of protecting company data is important to comply with government or contractual mandates.

Purpose

This policy defines responsibilities and roles for instilling information security awareness among all information resource owners, managers, service providers and users.

Audience

The company Awareness & Training applies to all individuals within the Company enterprise.

Awareness and Training Policy

- All must be well informed of their responsibilities as Information Owners, Managers, Users, and Service Providers.
- In cooperation with the training office, the company Information Security Officer is responsible for managing a training and awareness program for all individuals of the company and for consulting with members of the company on information security issues.
- Training classes and materials will be offered to instil the importance of appropriate information handling and to explain the implications of this policy.
- Training will be offered at least annually to all employees using various means online, classroom, posters, direct communication.
- Training should include specific information on the use of security precautions such as encryption, anti-viral tools, backup procedures, physical security and awareness of social engineering tactics.
- The company Security Officer is responsible for maintaining the security program, which makes the information resources described in this policy available to the company individuals.
- Managers and responsible for seeing that their employees take advantage of available security awareness resources.
- Information owners and vendors must become familiar with standard information security principles and procedures as they apply to the information resources under their care.

Disciplinary Actions for Violations

Any applicant who provides misleading, erroneous or wilfully deceptive information to company on an employment form or resume or in a selection interview is immediately eliminated from further consideration for employment with company.

Vendor Access Policy

Introduction

Vendors play an important role in the support of hardware and software management, and operations for company. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors, they can modify environmental systems, and reset alarm thresholds. Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and embarrassment to company.

Purpose

The purpose of the company Vendor Access Policy is to establish the rules for vendor access to company information resources and support services, vendor responsibilities, and protection of company information.

Audience

The company Vendor Access Policy applies to all individuals that are responsible for the installation of new Information Resources assets, and the operations and maintenance of existing information resources and who do or may allow vendor access for maintenance, monitoring and troubleshooting purposes.

Vendor Access Policy

- Vendors must comply with all applicable company policies, practice standards and agreements, including, but not limited to
    - Safety Policies
    - Privacy Policies
    - Security Policies
    - Auditing Policies
    - Software Licensing Policies
    - Acceptable Use Policies

- Vendor agreements and contracts must specify
    - The company information the vendor should have access to
    - How company information is to be protected by the vendor
    - Acceptable methods for the return, destruction or disposal of company information in the vendor's possession at the end of a contract
    - The vendor must only use company information and information resources for the purpose of the business agreement
    - Any other company information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others

- Company will provide an IT point of contact for the vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.
- Each vendor must provide company with a list of all employees working on the contract. The list must be updated and provided to company within 24 hours of staff changes.
- Each on-site vendor employee must acquire a company identification badge that will be displayed at all times while on company premises. The badge must be returned to company when the employee leaves the contract or at the end of the contract.
- Each vendor employee with access to company sensitive information must be cleared to handle that information.
- Vendor personnel must report all security incidents directly to the appropriate company personnel.
- If vendor management is involved in company security incident management the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable company change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate company management.

- All vendor maintenance equipment on the company network that connects to the outside world via the network, telephone line, or leased line, and all company IR vendor accounts will remain disabled except when in use for authorized maintenance.
- Vendor access must be uniquely identifiable and password management must comply with the company Password Practice Standard and Admin/Special Access Practice Standard. Vendor's major work activities must be entered into a log and available to company management upon request. Logs must include, but are not limited to, such events as personnel changes, password changes, project milestones, deliverables, and arrival and departure times.
- Upon departure of a vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to company or destroyed within 24 hours.
- Upon termination of contract or at the request of company, the vendor will return or destroy all company information and provide written certification of that return or destruction within 24 hours.
- Upon termination of contract or at the request of company, the vendor must surrender all company Identification badges, access cards, equipment and supplies immediately. Equipment and/or supplies to be retained by the vendor must be documented by authorized company management.
- Vendors are required to comply with all laws and company auditing requirements, including the auditing of the vendor's work.
- All software used by the vendor in providing service to company must be properly inventoried and licensed.
- If vendors are logically connected (connected Entity) to the companies network then the third party access procedures must be followed. This includes vendor business case for connection, a due-diligence process, proper information risk assessment, assigned owners and management approval process.
- All vendors will be monitored by the company to validate that they comply with the necessary compliance mandates as required.
- The list of such connected entities must be maintained and updated with proper network and security related information.

Disciplinary Actions for Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of company information resources access privileges, civil, and criminal prosecution.

System Development Policy

Introduction

The number of computer security incidents and the resulting cost of business disruption and service restoration continue to escalate. Implementing solid security policies, blocking unnecessary access to networks and computers, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce the risk and drive down the cost of security incidents.

Purpose

The purpose of the System Development Policy is to describe the requirements for developing and/or implementing new software in the company information technology resources.

Audience

The company System Development Policy applies equally to all individuals that use any company information technology resources.

System Development Policy

- IT is responsible for developing, maintaining, and participating in a System Development Life Cycle (SDLC) for company system development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this plan should address the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; general design; detail design; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before it is used for critical company information.
- All production systems must have designated owners and custodians for the critical information they process. IT must perform periodic risk assessments of production systems to determine whether the controls employed are adequate.
- All production systems must have an access control system to restrict who can access the system as well as restrict the privileges available to these users. A designated access control administrator (who is not a regular user on the system in question) must be assigned for all production systems.
- Where resources permit, there should be a separation between the production, development, and test environments. This will ensure that security is rigorously maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems. Likewise, all production software testing must utilize sanitized information.
- All application-program-based access paths other than the formal user access paths must be deleted or disabled before software is moved into production.

Disciplinary Actions for Violations

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants. Additionally, individuals are subject to loss of company information technology resources access privileges, civil, and criminal prosecution.

Appendix A

Detailed Document Revision Log

Version	Revision Date	Revised by	Comments
1.2	16 August 2016	Shane Wills	

TERMS OF USE – PLUSONE

AGREEMENT

By registering for the service and accessing the site you agree that you have read, understood and accepted these terms and conditions ("Terms") and agree to be bound by them.

We may change these terms or the charges at any time and any changes will be effective from the time they are posted on the site or are otherwise notified to you.

These terms record the entire agreement, and prevail over any earlier agreement between you and us. Except as otherwise provided in these terms, variation is only effective if signed by both PlusOne and you.

1. DEFINITIONS

1.1 In these Terms:

"Accounts Payable Invoices" means your accounts payable invoices to be processed as part of the Service;

"Charges" means the charges for the Implementation Services and for the Processing Services as part of providing the Service as set out initially in the Customer Proposal, and subject to change from time to time on prior notice to you;

"Confidential Information" means the confidential information relating to the subject matter of this agreement and includes:
(a) confidential information relating to the design, specification and content of the Service and the Site;
(b) confidential information relating to the Information; and
(c) information relating to the terms upon which the service is provided to you.

"Customer Proposal" means the proposal prepared by Sublime Streamline Ltd its reseller or agent for the provision of the service and accepted by you;

"Exceptions" mean any accounts payable Invoices forming part of the information which have failed to be validated in accordance with your specified business rules incorporated in the site;

"ERP System" means your enterprise resource planning system, accounts payable system or other accounting software into which all validated invoice records are to be exported from time to time;

"Implementation Services" means the initial customisation of the site for your use and initial implementation of your specified business rules to be applied in the validation of your information including any subsequent changes requested by you from time to time;

"Information" means any data, in any format, document, email, information entered, scanned or uploaded to the site or otherwise provided to PlusOne by you or on your behalf for the purpose of using the service including the accounts payable invoices and the validated invoice records;

"Intellectual Property Rights" mean all intellectual property rights including without limitation,
(a) patents, trademarks, copyright, registered designs, trade names, symbols and logos; and
(b) Tools, templates, techniques, computer program code, trade secrets, information or logical sequences (whether or not reduced to writing or other machine or human readable form);

"Minimum Volume" means the minimum number of accounts payable Invoices to be processed through the site on a monthly basis during the term as set out in the 'Authority to Proceed';

"PlusOne", "us", "our" or "we" means Sublime Streamline Limited, and its duly authorised licensees;

"Processing Services" means any electronic or manual manipulation of your Information including data recognition, data capture, data validation and exception handling services provided by us to you as part of the service;

"Service" means the online accounts payable service available via the site including the Implementation services and the processing services;

"Site" means our website (www.sublimeplusone.net) and all related systems, files, components and programs, or any part of it;

"Term" means the term you have agreed to subscribe to the service;

"User ID" means your user name and your password ("Password");

"Validated Invoice Records" means the electronic record of the accounts payable invoices created by us as a result of the processing services which has been validated in accordance with your specified business rules;

"Working Day" means any day other than a Saturday, Sunday or Public holiday in New Zealand;

"You" and "Your" means:

- the business entity registered to use the services under that subscriber name ("Subscriber") and
- any person or entity authorised by or on behalf of the Subscriber to use the service from time to time ("Registered User");

2. LICENCE

2.1 We give registered users and subscribers a non-exclusive, non-transferable licence to access the site and use the service strictly for the internal business purpose of the subscriber during the term.

2.2 You may not use the service for the benefit of any other third party.

3. YOUR INFORMATION

3.1 You agree to provide true and complete information about yourself and your organisation, and to let us know whenever any of your registration information changes. You confirm that you have authority to use the site.

3.2 Your information is your property. You license that Information to us so that we can provide the services to you. You undertake that the information provided to us or uploaded to the site does not infringe any person's intellectual property rights and is not otherwise illegal, fraudulent or defamatory.

3.3 You are responsible for resolving all exceptions in a timely manner and exporting all validated invoice records to your ERP System on a frequent basis.

3.4 While we use our best commercial efforts to prevent data loss, including backing up our own data, which may include the Information in original or amended form and the validated invoice records, we do not guarantee that there will be no loss of information. You must maintain back-up copies of your information and, once exported, all validated invoice records.

4. USER ID

4.1 You agree that you are solely responsible for all use of your User ID, you will change your password if we request you to do so and you will not gain or try to gain unauthorised access to the site.

4.2 The subscriber is responsible for access rights of registered users and for ensuring that user IDs of all registered users are kept secure and confidential.

4.3 The subscriber can set administration rights to the site, add, vary and delete any registered user and control the rights and permissions of any registered user using the site.

4.4 You must notify us immediately if there has been any unauthorised access to the site or if your User ID has been disclosed to a third party.

5. RESTRICTIONS ON USE

5.1 As a condition of using the service and accessing the site, you must not:

a. attempt to undermine the security or integrity of PlusOne's computing systems or

networks or, where the service is hosted by a third party, that third party's computing systems and networks;

b. use, or misuse, the service in any way which may impair the functionality of the services or site, or other systems used to deliver the service or impair the ability of any other user to use the service or site;

c. attempt to gain unauthorised access to any materials other than those to which you have been given express permission to access or to the computer system on which the service is hosted;

d. transmit, input or upload onto the site any files that may damage any other person's computing devices or software, content which may be obscene, offensive, upsetting or defamatory, or material or Information which infringes the intellectual property rights of any other person or otherwise does not comply with all applicable laws; and

e. attempt to modify, copy, adapt, reproduce, disassemble, decompile or reverse engineer any computer programs or software used to deliver the Service or to operate the Site except as is strictly necessary to use either of them for normal operation.

5.2 We reserve the right to:

a. place restrictions on the data size of Information transmitted to us and/or uploaded on the site, including traffic volumes and connection times to and from the site;

b. modify the site and change the URL address of PlusOne's server or hosted site.

5.3 While we use our best commercial efforts in providing the service, we do not guarantee or warrant that the use of the service or access to the site will be continuous or fault free.

6. PAYMENT

6.1 The charges are set out in the customer proposal, as varied by us from time to time by prior notice to you.

6.2 You undertake to ensure that not less than the minimum volume is processed through the site on a monthly basis during the term.

6.3 All charges are in New Zealand dollars and stated as exclusive of goods and services tax (GST) under the Goods and Services Tax Act 1985 and you agree to pay GST and any other taxes which do not relate to our income.

6.4 All charges must be paid on the payment dates agreed in the customer proposal, or, if no dates have been agreed, the 20th of the month following the invoice date.

6.5 You must pay us interest on any amount due and not paid by the due date at the rate of 15% per annum, calculated on a daily basis from the due date until the date of actual payment. We may also charge you for any debt collection agency fees which are incurred due to non-payment.

7 INTELLECTUAL PROPERTY RIGHTS

7.1 All intellectual property rights to the service and the site including all software and documentation associated with the site and any subsequent modifications and improvements belong to us or our authorised licensors.

8. CONFIDENTIALITY

8.1 Each party must not, without the prior written approval of the other party, disclose the other party's confidential information, and it must ensure that its employees and subcontractors comply with this obligation.

8.2 A party will not be in breach of this provision in circumstances where it is legally compelled to disclose the other party's confidential Information or where such information has become publicly available other than by a breach of this agreement.

8.3 This section shall survive termination of these Terms.

9. DISCLAIMER

9.1 You acknowledge that the use of the service and access to the site, and all related features available through the site are provided:

- on an "as is" and "as available" basis,
- at your sole risk and
- without representations or warranties of any kind, either express or implied, and all warranties, whether express or implied, are excluded including implied warranties of merchantability and fitness for a particular purpose.

9.2 In no circumstances (including negligence) will PlusOne, or any of our licensors or licensees, our related companies and affiliates or our or their officers, employees, advisers, partners, agents or suppliers, be liable for any:

- sort of damages that result from:
  - any of your Information,
  - your reliance on the site, or
  - the use of or access to, or the inability to use or access the site, or the loss of any data or Information;

- Indirect damage (including punitive damages), loss (including loss of use, data, profits, business or any economic loss) or cost (including legal and lawyer/client costs) caused or contributed to by us or them in relation to these terms.

9.3 You warrant that you are using this site or the service for the purposes of a business, and acknowledge and agree that the Consumer Guarantees Act 1993 does not apply.

10. LIMITATION OF LIABILITY

10.1 Our total aggregate liability to you or anyone else using the service or the site in respect of any one incident or series of connected incidents, for damages, losses, and causes of action (whether in contract, tort, including negligence, under statute or otherwise), will not exceed the total charges actually paid by you to us in the 12 months preceding the month in which the liability arises.

10.2 This limitation of liability extends to our licensors, related companies and affiliates and each of our or their officers, employees, advisers, partners, agents or suppliers.

10.3 No claim will be valid unless you give PlusOne written notice of the claim within 6 months after you become aware or should have become aware of the circumstances giving rise to such claim.

11. INDEMNITY

11.1 You agree to indemnify us and keep us indemnified against any loss, claim or demand (including any reasonable lawyer and own client costs) arising in relation to

- any breach by you of these terms,
- any act or omission for which you are responsible,
- non-payment of any charges when they become due,
- any Information and data provided by you,
- your use of the site or the service,
- any infringement by you of the rights of any other person.

11.2 This indemnity extends to our licensors, licensees, related companies and affiliates and each of our or their officers, employees, advisers, partners, agents or suppliers.

12. SUSPENSION OF SERVICES

12.1 These terms will apply from the date you first access the site, or you have registered as a subscriber or registered user, whichever is the earlier, and continue for the term.

12.2 PlusOne may immediately suspend your access to the site and/or use of the service or access to the information or terminate your registration as a registered user or a Subscriber:

- if you breach any of these terms,
- if we think that you have misused the site,
- if your registration information is, or we think that it is, untrue, incomplete or not

current,

- if you are or become insolvent or bankrupt, or if you make an assignment for the benefit of or enter into or make any arrangement or composition for the benefit of your creditors, or if you go into receivership or have a receiver, trustee and manager (or any of them) (including a statutory manager) appointed in respect of all or any of your property, or
- at any time by giving you not less than 30 days' prior notice.

13. EFFECT OF TERMINATION

13.1 On suspension or termination of your registration all licences granted under these terms will end and you may not use the site. On termination you will remain liable for any accrued charges which become due for payment before or after termination.

13.2 Terms intended to apply after termination of your registration will continue to apply.

14. NOTICES

14.1 We may give notices to you by email or by regular mail to your address. You may only give notice to us at enquiries@sublimegroup.net, or by regular mail to PO Box 340-118, Birkenhead, Auckland 0746. Notices will be deemed delivered in the case of regular mail 2 working days after (but exclusive of) the day of mailing and in the case of email notice on the date shown on our system of sending our email to you or our system's receipt of your email to us (as the case may be).

15. LINKING

15.1 We have not reviewed and are not responsible for any of the sites linked to the site. You may not link to the site (including framing, alteration of contents of the site, re-branding of content, use of metatags or hidden text techniques) without our written consent.

16. JURISDICTION

16.1 These terms, the service and the site are governed by New Zealand law.

17. DISPUTE RESOLUTION

17.1 If any dispute arises in relation to these terms, any party may notify the other in writing of the dispute and request resolution. The parties will then try to resolve the dispute by negotiation, mediation or other alternative resolution techniques. If the dispute is not resolved within 14 days of the date of receipt of the notice any party may refer it to be finally resolved by arbitration under the Arbitration Act 1996. The arbitration will be held in Auckland.

18. GENERAL TERMS

18.1 We will not be liable for any failure or delay in performing our obligations under these terms if the failure or delay arises directly or indirectly from a cause reasonably unforeseeable or beyond our control.

18.2 Your rights and obligations under the terms may not be assigned, transferred or otherwise disposed of in any way by you. We may assign any or all of our rights and obligations under these terms to any person.

18.3 No delay or failure by us to act is a waiver. No waiver is effective unless it is in writing. A waiver of a breach is not a waiver of any other breach.

18.4 The benefit of the disclaimers, exclusions and limitations in these terms are extended to our licensees with whom you may have contracted to provide the service to you pursuant to the Contracts (Privacy) Act 1982.