specialist **mail** services
your boutique mailhouse

DATA POLICY & PROTECTION PLAN

2020

Unit 2/42 Collingwood St, Osborne Park WA 6017 **T:**(08) 9443 3355 **E:** smail@specialistmail.com.au **W:** www.specialistmail.com.au
Eric Preston Pty Ltd trading as Specialist Mail Services ABN 66 008 753 348

specialist**mail** services
your boutique mailhouse

Data Protection Plan

Date:	01/09/2020	Author:	Chris Rinaldi
Client:	Specialist Mail Services	Ref IDs:	
Next Review:	24/03/2021		

Document Distribution

Name	Position	Company

Data Protection Plan:

This document identifies steps taken by Specialist Mail Services to identify methods to ensure the Protection and integrity of data within the Specialist Mail Services environment.

1. Antivirus:

Specialist Mail Services run Trend Micro Worry-Free Business Services. This is configured and maintained by Torque IT.

2. Firewall:

Specialist Mail Services operate a TP link Archver VR 1600v in conjunction with an EdgerouterX with rules to ensure secure access via VPN and restriction on accepted traffic connections to site.

3. Device Firmware:

Specialist Mail Services has a set schedule for device update checks:

Device	Firmware Version	Last Update Review	Scheduled Review
NAS – SM-NAS	Current 4.3.6.0875 Latest 4.4.1.1216	01/04/2020	01/04/021
PC – SMS-PC01	Current: 02.02.04 Rev.A Latest: 02.10.00 Rev.A	01/04/2020	01/04/021
PC – SMS-PC02	Current: 02.02.04 Rev.A Latest: 02.10.00 Rev.A	01/04/2020	01/04/021
PC – SMS-PC03	Current: 02.02.04 Rev.A Latest: 02.10.00 Rev.A	01/04/2020	01/04/021
PC – SMS-PC04	Current: 02.02.04 Rev.A Latest: 02.10.00 Rev.A	01/04/2020	01/04/021
PC – SMS-PC05	Current: 02.02.04 Rev.A Latest: 02.10.00 Rev.A	01/04/2020	01/04/021
Router – Netgear NightHawk R6700	Current V1.0.1.47 Latest V1.0.1.56	01/04/2020	01/04/021

4. File Storage:

Specialist Mail Services utilise Dropbox linked to unique accounts to ensure the security of file storage.

Staff access is controlled to match their job roles, allowing access only to required folders.

Dropbox retains deleted or changed files for an additional 120 days, ensuring recovery of data if required.

Specialist Mail Services is using Probax to back up their Dropbox storage. Currently 3 accounts are being backed up, each account has the following:

1. 100 GB of backup storage
2. 2 Years of Retention
3. Restore points
    a. 7 Daily
    b. 12 Monthly
    c. 2 Yearly

5. File Transfer:

Specialist Mail Services has two secure file transfer options.

1. Dropbox as a secure file transfer solution. Each customer is given a folder shared only to confirmed and requested members of that company to allow for secure upload of customer data to Specialist Mail Services. The "SMS Clients" files have an automatic removal period of 60 days after upload.

2. 7zip as a secure file transfer solution. Each customer is sent an encrypted zipped file with data and proofs. Passwords are sent in a separate email.

6. Email Security:

Specialist Mail Services uses the mail scanning solution CleanMail Anti-Spam/AntiVirus to reduce fraudulent and malicious email traffic both in and outbound.

7. Physical Site Security:

Specialist Mail Services restricts access to site and equipment with the following methods:

- Public and visible single entry/exit with auto entry/exit alert.
- Deadbolts for office lock down
- Delivery Entry/Exit fitted with NO ENTRY barrier and security deterrent
- External devices Exclusion Policy
- Secure IT data cabinet

8. Mailing Quality Control:

To ensure the integrity of recipient information Specialist Mail Services uses the following processes and technologies:

- Intel Barcode scanning software
- DS 200 Inserting Machines (x2) – Double Detection Software Features – Electronic & Mechanical
- Samples of Personalised Forms provided for review and approval prior to printing
- Printed Envelopes – Random manual validation checks

9. VPN

Using OpenVPN configuration setup on the Edgerouter and the OpenVPN client setup on each remote device. The VPN uses a separate VLAN, making it easy to identify which devices are connecting to the network remotely.

Privacy Policy

Specialist Mail Services is committed to providing quality services to you and this policy outlines our ongoing obligations to you in respect of how we manage your Personal Information.

We have adopted the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) (the Privacy Act). The NPPs govern the way in which we collect, use, disclose, store, secure and dispose of your Personal Information.

A copy of the Australian Privacy Principles may be obtained from the website of The Office of the Australian Information Commissioner at www.aoic.gov.au

What is Personal Information and why do we collect it?

Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect include: names, addresses, email addresses, phone and facsimile numbers.

This Personal Information is obtained in different ways including by email, our secure storage solution, from your website, and documentation you have provided to us. We don't guarantee website links or policy of authorised third parties.

We collect your Personal Information for the primary purpose of providing our services to you. We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure.

Sensitive Information

Sensitive information is defined in the Privacy Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information.

Sensitive information will be used by us only:

- For the primary purpose for which it was obtained
- For a secondary purpose that is directly related to the primary purpose
- With your consent; or where required or authorised by law.

Third Parties

Where reasonable and practicable to do so, we will collect your Personal Information only from you. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party.

Disclosure of Personal Information

Your Personal Information may be disclosed in a number of circumstances including the following:

- Third parties where you consent to the use or disclosure; and
- Where required or authorised by law.

Security of Personal Information

Your Personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorized access, modification or disclosure.

When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to delete and or destroy your Personal Information.

Access to your Personal Information

Specialist Mail Services will not charge any fee for your access request, but may charge an administrative fee if additional work is required prior to providing your Personal Information.

In order to protect your Personal Information we may require identification from you before releasing the requested information.

Policy Updates

This Policy may change from time to time and is available on request.

Last Update: 30/08/2018

Review: 01/04/2020

Next Review: 01/04/2021

Privacy Policy Complaints and Enquiries

If you have any queries or complaints about our Privacy Policy, please contact us at:

Specialist Mail Services

Unit 2, 42 Collingwood Street

Osborne Park WA 6017

Acceptable Use Policy

Author: Chris Rinaldi – Torque IT

Date Reviewed: 24/03/2020

Review History				
Name	Department	Role/Position	Date reviewed	Signature
Chris Rinaldi	Torque IT	Contractor	17/08/2018	C.Rinaldi
Chris Rinaldi	Torque IT	Contractor	26/02/2019	C.Rinaldi
Chris Rinaldi	Torque IT	Contractor	24/03/2020	C.Rinaldi

Approval History				
Name	Department	Role/Position	Date approved	Signature
Suzanne Zollo	Special Mail Services	Manager	01/04/2020	S. Zollo

1. Overview

The purpose of this policy is to establish acceptable and unacceptable use of electronic devices and network resources at Specialist Mail Services in conjunction with its established culture of ethical and lawful behavior, openness, trust, and integrity.

Specialist Mail Services provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives and must manage them responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

2. Scope

All employees, contractors, consultants, temporary and other workers at Specialist Mail Services, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by Specialist Mail Services, or to devices that connect to a Specialist Mail Services network or reside at a Specialist Mail Services site.

3. Policy Statement

3.1. General Requirements

3.1.1. You are responsible for exercising good judgment regarding appropriate use of Specialist Mail Services resources in accordance with Specialist Mail Services policies, standards, and guidelines. Specialist Mail Services resources may not be used for any unlawful or prohibited purpose.

3.1.2. For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic per the Audit Policy. Devices that interfere with other devices or users on the Specialist Mail Services network may be disconnected. Information Security prohibits actively blocking authorized audit scans. Firewalls and other blocking technologies must permit access to the scan sources.

3.2. System Accounts

3.2.1. You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

3.2.2. You must maintain system-level and user-level passwords in accordance with the Password Policy.

3.2.3. You must ensure through legal or technical means that proprietary information remains within the control of Specialist Mail Services at all times. Conducting Specialist Mail Services business that results in the storage of proprietary information on personal or non- Specialist Mail Services controlled environments, including devices maintained by a third party with whom Specialist Mail Services does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by Specialist Mail Services, or its customer and partners, for company business.

3.3. Computing Assets

3.3.1. You are responsible for ensuring the protection of assigned Specialist Mail Services assets that includes the use of computer cable locks and other security devices. Laptops left at Specialist Mail Services overnight must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of Specialist Mail Services assets to your direct supervisor or Manager.

3.3.2. All PCs, PDAs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

3.3.3. Devices that connect to the Specialist Mail Services network must comply with the Minimum Access Policy.

3.3.4. Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, asset management and device tracking software.

3.4. Network Use

You are responsible for the security and appropriate use of Specialist Mail Services network resources under your control. Using Specialist Mail Services resources for the following is strictly prohibited:

3.4.1. Causing a security breach to either Specialist Mail Services or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized; circumventing user authentication on any device; or sniffing network traffic.

3.4.2. Causing a disruption of service to either Specialist Mail Services or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.

3.4.3. Introducing honeypots, honeynets, or similar technology on the Specialist Mail Services network.

3.4.4. Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.

3.4.5. Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.

3.4.6. Use of the Internet or Specialist Mail Services network that violates the employment terms, Specialist Mail Services policies, or local laws.

3.4.7. Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers.

3.4.8. Port scanning or security scanning on a production network unless authorized in advance by Information Security.

3.5. Electronic Communications

The following are strictly prohibited:

3.5.1. Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that Specialist Mail Services policies against harassment or the safeguarding of confidential or proprietary information.

3.5.2. Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.

3.5.3. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

3.5.4. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

3.5.5. Use of a Specialist Mail Services e-mail or IP address to engage in conduct that Specialist Mail Services policies or guidelines. Posting to a public newsgroup, bulletin board, or listserv with a Specialist Mail Services e-mail or IP address represents Specialist Mail Services to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

3.5.6. Use of personal or external electronic or any other type of recording devices on the print floor. Includes, but not limited to, mobile phones, cameras, audio recorders and video devices. All devices are to be restricted to the office, breakroom or secured in a company locker or equivalent location identified by the office manager.

4. Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Specialist Mail Services.

Definitions

Term	Definition
honeypot, honeynet	Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
Spam	Electronic junk mail or junk newsgroup postings. Messages that are unsolicited, unwanted, and irrelevant.

Revision History

Date of Change	Responsible	Summary of Change
17/08/2018	Chris Rinaldi	Policy created
24/03/2020	Chris Rinaldi	Update of review dates and filename of document to current year.

specialist mail services
your boutique mailhouse

SMS Breach Action Plan

Reviewer:	Suzanne Zollo
Review Date:	01/04/2020
Updated:	01/04/2020 – Member 3 Team Member amended
Next Review Date:	01/04/2021

Data Breach response team members:

- Member 1 – Primary Breach Officer – Suzanne Zollo – Executive Manager
- Member 2 – Secondary Officer – Chantelle Nathan – Operations Manager
- Member 3 – Team Member – Anais Colas – Production Manager
- Member 4 – ICT Officer – Torque IT Management

Breach Plan Testing:

- Testing occurs annually
- Testing facilitated by Suzanne Zollo and Torque IT
- Test results kept by SMS and Torque IT

Action Plan:

Step 1: Identify the Breach and contain

External Support identified at this stage, if required.

Confirm spokesperson for any communication

Step 2: Assess the risks for individuals associated with the breach

Complete Personal Data Security Breach Form:

Date/time of Breach

Cause and extent

Type of information

Step 3: Breach notification

Notification of Customers

Incident Report Completed

Step 4: Review the incident and take action to prevent future breaches

Review of incident procedure

Identification of breach point and action plan to avoid in future.

specialist **mail** services
your boutique mailhouse

Checklist	YES/NO
How is a data breach identified?	
Does your staff know what to do if they suspect a data breach has occurred?	
Who is ultimately responsible for your entity's handling of a data breach in accordance with the plan? – Suzanne Zollo	
Who is on your response team? – Chantelle / Suzanne	
Do you need to include external expertise in your response team, for example ICT Officer	
Do they know their roles and what to do?	
Have you set up clear reporting lines?	
When do you notify individuals affected by a data breach?	
What records will be kept of the breach and your management of it?	
Does your plan refer to any strategies for identifying and addressing any weaknesses in data handling that contributed to the breach?	

specialist **mail** services
your boutique mailhouse

Specialist Mail Standard Operating Environment

All PCs purchased or setup from date of review to be compliant with below specifications.

Date of Review: 01/04/2020

Date of next Review: 01/04/2021

Naming convention: SMSPC## where ## is a unique number.

Hardware:

- RAM: 16GB
- CPU: intel i5-9th gen or newer
- Disk: 256GB SSD

OS:

- Windows 10 Pro

Additional Software requirements:

- Microsoft Word 2013+
- Microsoft Office 2013+
- Microsoft Excel 2013+
- Trend Micro Worry-Free Business Security Agent
- Torque IT Asset Scan
- Bomgar remote access server

Optional Software:

- TeamViewer Server
- Adobe InDesign

Domain:

- None, workgroup only

Local Admin:

- Account "SMSadmin" password stored securely with Torque IT

Reviewed By: _____ Signed:_____

specialist **mail** services
your boutique mailhouse

Compliance Review Master List

Specialist Mail Services

Document	Last Review	Reviewer	Next Review
SMS – Data Protection Plan	01/04/2020	Suzanne Zollo	01/04/2021
SMS – Acceptable Use Policy 2018	01/04/2020	Suzanne Zollo	01/04/2021
SMS – Breach Action Plan Template 2018	01/04/2020	Suzanne Zollo	01/04/2021
SMS - Breach Notification Letter Template 2018	01/04/2020	Suzanne Zollo	01/04/2021
SMS - Breach Notification Template 2018	01/04/2020	Suzanne Zollo	01/04/2021
SMS - DataSecurityBreachFormInternal 2018	01/04/2020	Suzanne Zollo	01/04/2021
SMS - Privacy Policy 2018	01/04/2020	Suzanne Zollo	01/04/2021
SMS - Standard Operating Environment 2018	01/04/2020	Suzanne Zollo	01/04/2021