PREFACE

iPipeline Canada takes its client's security and privacy concerns seriously. In an ever changing landscape of security risks and compliance demands, we take the utmost care to ensure our client's data is kept secure in a seamless fashion so that our users are free to concentrate their attention on their business.

This security statement has been created to provide transparency to our users about the practices and procedures that are currently in place to ensure the security of our client's information, which is at the heart of their business.

CONTENTS

APPLICATION AND USER SECURITY

- **SSL/TLS Encryption:** All web traffic for the WealthServ application occurs over secured, encrypted Secure Socket Layer (SSL) / Transport Layer Security (TLS) connections. This ensures that the information transmitted between your browser and our servers is safe and secure and can only be read by the intended recipients.
- **sFTP / SSH:** All files delivered to, and available for pick up from our FTP site takes place over a secured Secure Shell (SSH) connection. Similar to SSL/TLS, this ensures that the files transmitted to or from the client and the server are safe and secure.
- **User Authentication:** All client data stored within the WealthServ database servers are logically separated into their own database. User accounts have unique usernames and passwords that must be entered each time a user logs on.
- **Authorization:** Within WealthServ, all users are assigned a role which dictates the types of information they have access to and activities they are able to perform. This allows administrative staff to ensure that the users of their system only have access to what they need to perform their job.
- **Privacy:** We have a comprehensive privacy policy that provides a very transparent view of how we handle your data, including how we use your data, who we share it with, and how long we retain it.

PHYSICAL SECURITY

- **Data Centers:** The WealthServ infrastructure is collocated at third party data centers. We own and manage all equipment located in these facilities.
- **Data Center Certifications:** Our data centers have achieved the following certifications: CSAE 3416, ISAE 3402, PCI Compliance, SSAE 16 SOC 1 and AT 101 SOC 2 Type 1. These certifications are updated on an annual basis. In addition, our production datacenter has been officially Tier III certified by the Uptime Institute.
- **Data Center Security:** Our data centers are staffed and monitored 24/7. Security guards patrol the premises regularly and the facility contains closed circuit video monitoring systems throughout the interior and exterior which is monitored 24/7 by datacenter staff as well as third party security firms. Dual factor authentication is required on all exterior doors and there is a single point of physical entry for clients protected by security staff behind bullet-resistant glass. Entrance is granted by a dual factor system – encrypted card access and biometric iris scanning. A secure turnstile prevents un-authorized access with anti-passback technology and man-trap functionality to prevent tail-gating. All interior doors are protected by a card access system. All equipment is stored in locked cages.
- **Environmental Controls:** Our data center is maintained at controlled temperatures and humidity ranges, which are continuously monitored for variance. The facility contains a comprehensive fire detection and suppression system that utilizes Novec 1230 gas and is supported by a 2-stage pre-action dry pipe water suppression system. For detection, ion based particle sensors are deployed above and below the 42" anti-static raised floor.
- **Location:** All client data is stored on servers located in Canada.

AVAILABILITY

- **Connectivity:** High availability network design with redundant production firewalls and switches utilizing layer 3 failover capabilities. Two fully independent network paths to the datacenter network core with automatic failover in the event of path unavailability. This is supported by a multi-homed, fully redundant Internet backbone.
- **Power:** Our datacenters meet the Tier III requirement of concurrently maintainable power and have multiple independent distribution paths to our equipment (A & B side power). All equipment is protected by a high capacity, uninterruptible power supply (UPS) system and diesel generators that are rated to provide power to the entire facility on a continuous duty basis.
- **Monitoring:** Internal and external monitors are in place to immediately notify WealthServ staff in the event of any downtime.
- **Disaster Recovery:** Warm disaster recovery facility is in place and backup data is shipped to this offsite facility on a daily basis.

NETWORK SECURITY

- **Firewall:** Enterprise grade firewalls protecting the entire WealthServ environment with a strict rule base (only allowing ports required for system functionality). Segregated DMZ network for web traffic and LAN network for backend processing of data.
- **Intrusion Prevention:** Intrusion Prevention System deployed on all web facing systems.
- **Patching:** Latest security patches are applied to all operating systems to mitigate newly discovered vulnerabilities.
- **Access Control:** Access to the environment is provided by SSLVPN utilizing Duo/OKTA MFA authentication. Role-based access is enforced for systems managed by authorized WealthServ staff.
- **Logging and Auditing:** Advanced firewall reporting and analytics. Management and monitoring of production firewalls and switches provided by skilled datacenter staff.
- **DDOS Mitigation:** DDOS detection and mitigation devices installed within the datacenter network core to significantly reduce the risk of denial of service attacks.
- **Antivirus:** Next-generation antivirus that blocks known threats and continuously analyzes data behaviour patterns to detect and block unknown threats.

STORAGE SECURITY

- **Backup and Replication:** Backups occur daily and all data is replicated offsite to our disaster recovery facility. Virtual Machines are replicated to a secondary Data Centre utilizing Site Recovery Manager and provides increased reliability in the event of a disaster.
- **Production Redundancy:** Data is stored on enterprise grade storage arrays utilizing redundant controllers and RAID technologies.
- **Encryption:** To protect data at rest, all data is encrypted using VM-level encryption with separate Key Management Server. All replication and backups are encrypted using AES-256 encryption.

ORGANIZATIONAL & ADMINISTRATIVE SECURITY

- **Employee Screening:** Criminal record background screening is performed on all employees. Confidentiality agreements are mandatory and all staff must physically signoff on policies and procedures.
- **Training:** All employees must undergo annual security training.
- **Service Providers:** Service providers are screened and bound under contract to appropriate confidentiality obligations.
- **Access:** Internal access to data, systems and environments is provided on a need-to-know / least privilege required basis.
- **Information Security Policies:** Internal information security policies are reviewed and updated on a regular basis.

HANDLING OF SECURITY BREACHES

Despite the numerous controls we have implemented to reduce the risk of a security breach, no method of data transmission or storage is completely secure. If WealthServ learns of a security breach, we will notify all affected clients so that they can take protective action. Notification procedures include email correspondence or a notice posted on our website. In addition, we will perform a root cause analysis to determine the source of the breach and take appropriate corrective action.

CLIENT RESPONSIBILITIES

A large component of keeping your data secure is ensuring you maintain the security of your account by using complex passwords and storing them securely. Having sufficient security on your own systems is also highly recommended. We utilize SSL to secure all transmission over the Internet; however, you must also ensure appropriate controls on computers accessing our systems are in place.Options for creating positive cash flow while building and maintaining your own electronic signature solution could be years in the making or not at all. Companies that build and maintain their own electronic signature solution generally do so for non-monetary reasons.