WILLIAMS ASSET MANAGEMENT WRITTEN INFORMATION SECURITY PROGRAM

TABLE OF CONTENTS

I. INTRODUCTION

II. OBJECTIVE

III. DEFINITIONS

IV. PURPOSE

V. SCOPE

VI. GOVERNANCE AND OVERSIGHT

VII. INTERNAL RISKS

VIII. EXTERNAL RISKS

This WISP applies only to the security of information relating to business conducted through Commonwealth Financial Network® (Commonwealth) or CES Insurance, Inc. WILLIAMS ASSET MANAGEMENT and Commonwealth are separate and unrelated entities.

I. INTRODUCTION

WILLIAMS ASSET MANAGEMENT, a MARYLAND-based company, adopted this Written Information Security Program (WISP) as part of its efforts to comply with the standards set forth in MA 201 CMR 17.00 and the data privacy requirements of all states in which WILLIAMS ASSET MANAGEMENT does business.

II. OBJECTIVE

WILLIAMS ASSET MANAGEMENT's objective in developing and implementing this WISP is to create effective administrative, technical, and physical safeguards for the protection of the personal information of clients and WILLIAMS ASSET MANAGEMENT users (as defined below), as well as to comply with obligations under all applicable federal and state laws and regulations. The WISP sets forth WILLIAMS ASSET MANAGEMENT's procedure for evaluating electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information.

III. DEFINITIONS

WILLIAMS ASSET MANAGEMENT users include all regular full- and part-time employees, as well as temporary employees, co-ops, interns, and third-party contractors and consultants of WILLIAMS ASSET MANAGEMENT and its affiliates.

Encryption is the process of transforming data into a form in which meaning cannot be assigned without the use of a confidential process or key.

Personal information is an individual's first name (or first initial) and last name in combination with any one or more of the following data elements: (a) social security number; (b) driver's license number or government-issued identification card or documents; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password, that would permit access to a financial account. This personal information does not include, however, information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

IV. PURPOSE

The purpose of this WISP is to:

- Ensure the security and confidentiality of personal information
- Protect against any anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud
- Ensure that WILLIAMS ASSET MANAGEMENT identifies and responds to breaches of personal information

V. SCOPE

In formulating this WISP, WILLIAMS ASSET MANAGEMENT has (1) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information; (2) assessed the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluated the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (4) designed and implemented safeguards to minimize those risks; (5) regularly monitored the effectiveness of those safeguards; and (6) determined when and how to respond to potential breaches of personal information.

VI. GOVERNANCE AND OVERSIGHT

WILLIAMS ASSET MANAGEMENT's Information Security and Privacy Committee is responsible for the following duties, including, but not limited to:

- Reviewing WILLIAMS ASSET MANAGEMENT's information security and privacy policies and procedures and recommending improvements and revisions thereto, as appropriate
- Reviewing, on a quarterly basis, information security and privacy incidents and Information Security reports
- Serving as a resource for WILLIAMS ASSET MANAGEMENT on information security and privacy issues
- Evaluating information security and privacy training needs
- Coordinating efforts to make information security and privacy more visible within the company

WILLIAMS ASSET MANAGEMENT has designated that its chief information security officer (CISO) will implement, supervise, and maintain the WISP. The CISO is responsible for the following:

- Overseeing the initial implementation of the WISP
- Performing regular testing of the WISP's safeguards
- Evaluating the ability of third-party service providers to implement and maintain appropriate security measures for the personal information to which WILLIAMS ASSET MANAGEMENT has permitted them access, consistent with applicable federal and state laws and regulations, and requiring such third-party service providers by contract to implement and maintain appropriate privacy and security measures
- Reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in WILLIAMS ASSET MANAGEMENT's business practices that may implicate the security or integrity of records containing personal information
- Conducting required training sessions for all WILLIAMS ASSET MANAGEMENT users on privacy and information security (All attendees at such training sessions are required to certify their attendance at the training and attest to their compliance with WILLIAMS ASSET MANAGEMENT's requirements for ensuring the protection of personal information.)

In carrying out these responsibilities, the CISO may delegate any or all of these tasks.

VII. INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, as well as evaluating and improving—where necessary—the effectiveness of the current safeguards for limiting such risk, the following measures are mandatory and are effective immediately:

Protection against internal threats

- **Communication.** A copy of this WISP will be distributed to each WILLIAMS ASSET MANAGEMENT user who shall, upon receipt of the WISP, acknowledge in writing that he or she has received a copy of the WISP.

- **Compliance.** All WILLIAMS ASSET MANAGEMENT users are required to comply with the provisions of the WISP. Any unauthorized use of personal information during or after employment may result in disciplinary action. Disciplinary actions may include termination of employment. In some cases, civil or criminal action may be pursued.

- **Collection.** The amount of personal information collected should be limited to that amount reasonably necessary to accomplish WILLIAMS ASSET MANAGEMENT's legitimate business purposes or to comply with applicable federal and state laws and regulations.

- **Access rights and controls.**

  - Access to records containing personal information shall be limited to those WILLIAMS ASSET MANAGEMENT users who are reasonably required to know such information in order to accomplish WILLIAMS ASSET MANAGEMENT's legitimate business purpose or to enable WILLIAMS ASSET MANAGEMENT to comply with applicable federal and state laws and regulations.

  - Access to electronically stored personal information shall be limited to those WILLIAMS ASSET MANAGEMENT users having a unique login ID. A re-login shall be required when a computer has been inactive for more than 10 minutes.

  - Electronic access to WILLIAMS ASSET MANAGEMENT's network and systems that contain personal information will be blocked after multiple unsuccessful attempts to gain access.

  - Current WILLIAMS ASSET MANAGEMENT users' passwords must be changed periodically.

  - Terminated WILLIAMS ASSET MANAGEMENT users are required to return all records containing personal information, in any form, that may at the time of such termination be in the former WILLIAMS ASSET MANAGEMENT user's possession (including all such information stored on laptops or other portable devices or media and in files, records, work papers, etc.).

  - Upon termination, a WILLIAMS ASSET MANAGEMENT user's physical and electronic access to personal information will be immediately blocked. Such terminated WILLIAMS ASSET MANAGEMENT user shall be required to surrender all keys, IDs, access codes or

badges, business cards, and the like that permit access to WILLIAMS ASSET MANAGEMENT's premises or information.

- Upon termination, a WILLIAMS ASSET MANAGEMENT user's remote electronic access to personal information will be disabled; his or her voice mail access, e-mail access, Internet access, and passwords will be invalidated.

- **Physical access controls.**

  - WILLIAMS ASSET MANAGEMENT users are prohibited from keeping open files containing personal information on their desks when they are not at their desks.

  - At the end of the workday, all files and other records containing personal information are required to be secured in a manner that is consistent with the WISP's rules for protecting the security of personal information.

  - Visitors must be registered and accompanied throughout the duration of their visit. Visitors are required to register at the reception desk, sign in, and display a clearly visible guest badge or tag throughout their visit.

- **Secure disposal.** Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies with Maryland law.

- **Incident response.**

  - WILLIAMS ASSET MANAGEMENT users are required to report any suspicious or unauthorized use of personal information to the Information Security department.

  - Whenever there is an incident that requires notification under applicable federal and state laws and regulations, the Information Security department will initiate a post-incident review of events and actions taken, if any, with a view to determining whether any modifications to security practices are necessary to improve the security of the personal information for which WILLIAMS ASSET MANAGEMENT is responsible.

- **Periodic review.** All security measures shall be reviewed at least annually or whenever there is a material change in WILLIAMS ASSET MANAGEMENT's business practices that may reasonably implicate the security or integrity of records containing personal information. The Information Security and Privacy Committee shall be responsible for this review and shall apprise the Risk Committee of the results of that review and any recommendations for improved security arising out of that review.

VIII. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information, as well as to evaluate and improve—where necessary—the effectiveness of the current safeguards for limiting such risks, WILLIAMS ASSET MANAGEMENT has implemented the following measures:

Protection against external threats

- **Firewalls and patching.** WILLIAMS ASSET MANAGEMENT employs reasonably up-to-date firewall protection and operating system security patches, which are designed to maintain the integrity of personal information, installed on all systems processing personal information.

- **Anti-malware.** WILLIAMS ASSET MANAGEMENT has reasonably up-to-date versions of system security agent software, which includes malware protection and up-to-date patches and virus definitions, installed on all systems processing personal information.

- **Encryption.** To the extent that is technically feasible, WILLIAMS ASSET MANAGEMENT encrypts all personal information stored on laptops and other portable devices, as well as records and files that contain personal information and are transmitted across public networks or wirelessly.

- **Authentication.** WILLIAMS ASSET MANAGEMENT has secure user authentication protocols in place, including (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; and (3) control of passwords to ensure that they are secure.

TECHN-4344-35038_02/18