The Arch MI Privacy and Security Program Summary

One of the most important assets of Arch U.S. MI Holdings Inc. and its subsidiaries ("Arch MI")[1] is the trust our business customers place in us to properly handle nonpublic personal information that is provided to, or acquired by, Arch MI in connection with the delivery of products and services. Arch MI is committed to protecting the privacy and the security of our customers' information. As part of that commitment, Arch MI will maintain the nonpublic personal information provided by our customers so that it is accurate, protected against manipulation and errors, secure from theft and free from unwarranted disclosure.

Maintaining Data Privacy

The Arch MI Privacy and Security Program Summary ("Privacy Summary") applies to the nonpublic personal information we will collect related to individual borrowers who receive financial products or services from our customers. Nonpublic personal information generally refers to information that can be used to identify or contact a specific borrower, such as loan application information, information from credit reporting agencies, information regarding the specific transaction and property information. This information is classified as Sensitive Personal Information and/or Confidential Information under the Arch Asset Management Standard. It is the policy of Arch MI to comply with all laws and regulations regarding use and disclosure of nonpublic personal information relating to individuals. Such information will be used solely to facilitate the products and services requested or as permitted by law. Arch MI may also acquire data from third-party sources, such as credit reporting agencies.

Whether in paper or electronic form, Sensitive Personal Information and Confidential Information are subject to physical, electronic and procedural safeguards and will be stored, transmitted and disposed of in accordance with the provisions of Arch's Global Privacy Policy. Arch MI restricts access to this information to just those employees who are specifically authorized to know the information in order to provide financial products and services.

Sensitive Personal Information and Confidential Information may be disclosed in connection with insurance underwriting, administration of the insurance transaction, reporting, investigating and preventing fraud or material misrepresentations, processing premium payments, handling insurance claims, administering insurance benefits and participating in related research projects or as otherwise required or specifically permitted by law or regulation. These disclosures typically are limited to the originator of the loan, the insured party and its agents, successors and assigns, credit reporting agencies, reinsurance companies and third parties that perform those services for Arch MI.

---

[1] Arch U.S. MI Holdings Inc. and subsidiaries are Arch Mortgage Insurance Company, Arch U.S. MI Services Inc., Arch Mortgage Guaranty Company, Arch Mortgage Assurance Company, United Guaranty Residential Insurance Company, United Guaranty Services, Inc. D/B/A Arch Fulfillment Services, and United Guaranty Residential Insurance Company of North Carolina.

Arch MI requires unaffiliated third parties that are given access to nonpublic personal information to sign written agreements requiring protection of the data and restricting the use of the information to those persons required to have access to the information in order to carry out the specified purpose of the agreement.

Maintaining Data Security

Arch MI has created a mature information security program with a “defense in depth” approach with regard to protecting its technology infrastructure and the information it contains. This includes both logical and physical components. Customers are offered a variety of options to transmit their data to Arch MI securely and once in our environment that data is appropriately protected.

The Demilitarized Zone (DMZ) is separated from the internet through the use of an external facing firewall/router. All traffic entering Arch MI’s protected internal network must pass through additional granular firewall rules.

Arch MI has implemented Intrusion Detection/Prevention Systems (IDS) to detect inappropriate behavior on the network. The IDS — augmented by additional relevant information — are monitored by trained security professionals.

To provide a layered defense against virus and malware attacks, Arch MI employs a robust combination of anti-virus and anti-malware systems, software and devices. All network traffic is scanned for malware and viruses as it enters or exits Arch MI’s network. Email, a common threat vector, is also scanned at the email gateway. Additionally, all Windows desktops and servers are equipped with anti-virus software.

Security and privacy are ingrained into our workforce. Before beginning work at Arch MI, all applicants must successfully pass an investigative background check. Current employees who are considered for promotion or transfer may be subject to an additional background investigation. Our workforce also participates in regular training, awareness programs and testing. However, we do not rely on training alone to protect against threats that include the introduction of potentially dangerous malware such as viruses and worms. End users are prevented from accessing potentially dangerous websites through the use of web-blocking technology.

Arch MI also employs restrictive access controls, rigorously enforcing the rule limiting access to data to a need to know basis. For Arch MI's remote employees, we additionally require multi-factor authentication before we will permit remote access to our network.

Like the network and applications, Arch MI’s physical plant is also secure. Only authorized individuals may enter areas where sensitive information is processed. Building access is restricted to employees with proper credentials. Visitors are required to sign in and obtain an identification badge. Security cameras are in place to monitor certain areas of the facilities. Arch MI’s data centers are physically secure and are equipped with raised floors, fire suppression, environmental monitoring, emergency power systems and leak detection.

When media containing private information are destroyed, it is Arch MI's policy that it is done securely. This includes paper documents which, per Arch's Global Records and Information Management Policy, are to be disposed of by a method appropriate to their content or level of confidentiality (i.e., shredded, recycled, deleted, etc.).

Through the layering of strong network protections, segmentation, physical and logical access controls and robust physical security, Arch MI provides excellent protection of information assets. We periodically assess whether these controls are operating as intended using both internal resources as well as independent third parties.

Like yours, our business changes constantly. The Privacy Summary will also change. Those changes will be reflected here.

For more information, contact corporate.compliance@archmi.com, or call 877-642-4642.