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 Non-Public Information ("NPI") we will collect related to individual borrowers who receive financial products or services from our customers. NPI 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 Personal Information and/or Confidential Information under the Arch's Global Privacy and Data Handling Policy. Arch MI's policy is to comply with all laws and regulations regarding use and disclosure of NPI 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, 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 and Data Handling 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.

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, and United Guaranty Services, Inc. DBA Arch Fulfillment Services.

Arch MI requires unaffiliated third parties that are given access to NPI 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 focused on a "defense in depth" approach to layering controls within its environment and following zero trust principles 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 granular firewall rules.

Arch MI has implemented Intrusion Detection/Prevention Systems ("IDS") and Network Detection and Response ("NDR") systems to detect inappropriate behavior on the network. These systems, augmented and correlated with additional relevant information, are monitored by trained security professionals 24/7.

To provide a layered defense against virus and malware attacks, Arch MI employs a robust combination of anti-virus and anti-malware systems. This includes file integrity monitoring and an endpoint detection and response ("EDR") platform that alerts and notifies security personnel of any unexpected behavior or potentially malicious files. Additionally, all network traffic is scanned for malware and viruses entering or exiting Arch MI's network and email, a common threat vector, is scanned at the email gateway to detect potential threats. Email security configurations are also in place both internally and externally to recognize and respond to email authorization standards that detect potentially malicious or unwanted traffic.

Security and privacy are ingrained into our workforce. Before beginning work at Arch MI, all applicants must successfully pass a background check. Our workforce also participates in regular security training courses, awareness programs and social engineering 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 using site blocking technology. Arch MI's workforce is required to present multi-factor authentication before accessing the Arch environment remotely.

Like the network and applications, Arch MI's physical locations are also secured. 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 sensitive areas and entrance/egress points of the facilities. Arch MI's data center is physically secure and is equipped with raised floors, fire suppression, environmental monitoring, emergency power systems and leak detection.

Arch also leverages various cloud services within its technology environment. Infrastructure as a Service (“IaaS”), Platform as a Service (“PaaS”) and Software as a Service (“SaaS”) are all services consumed by Arch. Additional considerations and controls are accounted for when leveraging cloud resources. Cloud configurations are monitored against the Center for Internet Security (CIS) benchmarks for infrastructure and platform services. Automated SaaS platform monitoring is also in place to track alignment with secure configurations for these services. Network communications to and from cloud resources occur over encrypted transmission channels.

When media containing Personal Information and Confidential Information is destroyed, Arch MI’s policy is that it is done securely. This includes paper documents that, in accordance 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, and those changes will be reflected here.

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