WEST CORPORATION
GLOBAL HR DATA PRIVACY STATEMENT SUMMARY

This statement describes how West Corporation and its subsidiaries and affiliates worldwide ("West") collect and use information about its employees and other personnel. This statement applies to West's global organization and provides a general notice of West's business practices. Specific questions in regards to this Statement should be directed to Amrik Mann at amann@west.com for EMEA and APAC, or Melissa Tejeda-Garza at mtejeda-garza@west.com for all remaining West locations. This notice is effective on March 20, 2018. The following summary provides the key points of the West statement. More complete information follows.

What Personal Data are collected?

- West collects Personal Data, including, when required, Sensitive Personal Data, about West personnel for administrative purposes or to conduct the business of the Company, such as application information, employment performance or disciplinary history.

How does West collect Personal Data?

- West collects Personal Data through the application process, whether online or in paper format. West also collects Personal Data upon hire through completion of employment documents including, but not limited to, tax and employee benefit documents.

How does West use Personal Data?

- West uses Personal Data to conduct its business of West and to comply with legal obligations.
- When West seeks to use Personal Data for a purpose incompatible with the original or other authorized purposes for which it was collected, West will give relevant personnel notice and (where feasible and appropriate) an opportunity to decline such uses.
- West may process Personal Data about its employees and other personnel for purposes connected with employment, including recruitment, benefits, and termination.
- Personal Data may also be used in connection with certain corporate transactions, to address governmental requests and requirements, and in connection with ongoing and prospective legal proceedings.

How can personnel update their Personal Data?

- West expects its employees and other personnel to report changes to their Personal Data to help maintain accurate, current and reliable data.
- Personnel may request to review Personal Data in their own personnel file and if necessary request corrections to such data.
- West maintains Personal Data only for as long as the data are necessary and relevant for legitimate business purposes.

Where does West Transfer Personal Data?

- Personal Data will be shared with third parties only for purposes provided in this statement, and as necessary to comply with a legal obligation of the company or when necessary for the performance of a contract between the data subject and the Company.
- West is an international company that shares data across its global operations consistent with its business purposes. West provides a rigorous, unified level of data protection across its operations, and in its dealings with its vendors. West enforces these obligations on its corporate affiliates through, in part, the use of European Union model contracts for data protection.
- West will not share information with service providers who do not guarantee adequate protection for Personal Data entrusted to them by West.

How does West secure its Personal Data?

- West's Information Security Policy and Standards Manual is available to West employees through the West Intranet home page and the West Legal Intranet site.
- West maintains reasonable and appropriate measures, including physical, electronic and procedural safeguards, to protect Personal Data from loss, misuse, unauthorized access or inadvertent destruction.
- West takes appropriate precautions to restrict access to Personal Data to only those personnel with a need to know and requires all employees to respect the privacy of Personal Data. Violations of this Statement can lead to appropriate employee discipline including separation from West.
- West personnel are responsible for maintaining information security, and must take all appropriate precautions and adhere to all data security policies.
- Employees must immediately report any breaches of confidentiality or security to breach@west.com.

Does West have a Data Protection Officer (DPO)?

- Europe's General Data Protection Regulation requires companies that process Europe-based personal data to appoint a DPO.
- West's DPO is Steven Taylor. He is located in EMEA and he can be contacted at steven.taylor@west.com.

Questions, Concerns, Disputes?

- Requests to access your Personal Data, concerns about inaccurate information or disputes regarding privacy and data protection issues should be referred to Amrik Mann at amann@west.com for EMEA and APAC, or Melissa Tejeda-Garza at mtejeda-garza@west.com for all remaining West locations. You may also contact privacy@west.com for any privacy and data protection matters.

WEST CORPORATION GLOBAL HR PRIVACY STATEMENT

INTRODUCTORY STATEMENT

In order to implement and promote compliance with the various privacy and data protections obligations of West Corporation and its subsidiaries (collectively, "West" or the "Company"), West has adopted this Global Privacy Statement (the "Statement"). The Statement is based on the privacy and data protection principles common to the countries in which West operates and is applied in light of our over-arching obligations to:

- comply with applicable law and regulation, including laws local to each jurisdiction in which West operates;
- preserve and secure the Personal Data of individuals, whether current or prospective clients, employees or others; and
- respect the privacy of our personnel.

West's employees and service providers must respect the privacy of Personal Data, and use reasonable and appropriate security safeguards to protect such data against loss and misuse as well as unauthorized access, disclosure, alteration or destruction.

This Statement is binding on all West personnel, including personnel from West subsidiaries and contractors, and shall be implemented globally throughout West.

- Appropriate disciplinary proceedings, including possible termination, are potential consequences of a failure to comply with this Statement. Any questions, requests, comments or concerns regarding this Statement may be addressed to Amrik Mann at amann@west.com for EMEA and APAC, or Melissa Tejeda-Garza at mtejeda-garza@west.com for all remaining West locations.

This statement may be updated from time to time. Any changes in how West handles Personal Data will be communicated to employees in advance of the change. The most current version of this statement is available on the West Intranet.

DEFINITIONS

For the purpose of this Statement, the following defined terms shall have the following meanings:

- **"Personal Data"** means any information relating to an identified or identifiable living natural person. "Personal Data" may include, for example, names, signatures, employee identification numbers, social security numbers, telephone numbers, insurance policy numbers, job titles, financial information, account numbers, or any other information that is capable of being associated with a particular identifiable individual. "Personal Data" does not include aggregate data where a person cannot be identified. "Personal Data" is broader than the term "Personal Information" as used in the Information Security Policy Manual.
- **"Sensitive Personal Data"** means data about children, financial information, health information (including PHI as defined by HIPAA), Social Security or other national

identification number, racial or ethnic origin, political opinions, religious beliefs, trade union membership, sex life, criminal convictions, and precise geolocation data.

SECTION 1. COLLECTION AND USE OF PERSONAL DATA

1.1 Personal Data

West limits the collection, usage, disclosure and retention of Personal Data relating to its personnel to that which is relevant and proportionate to its legitimate business purposes as set out in this Statement, or for those purposes subsequently authorized by the individual, or as required or permitted by law.

West collects, maintains and uses Personal Data, including when necessary Sensitive Personal Data, about West employees for administrative purposes, to conduct the business of West, to manage employer/employee relationships, to provide a safe workplace for employees, and to comply with legal and regulatory obligations. Such Personal Data may include, but is not limited to, any references obtained during recruitment, details of terms of employment, payroll details, tax and national insurance information, details of job duties, details of health and sickness absence records, information about performance, details of any disciplinary investigations and proceedings, training records, contact names and addresses, and other information voluntarily given to West or publicly available. Throughout their employment and for as long as is necessary after the termination of employment, West may process Personal Data about its employees for purposes connected with employment, including recruitment and termination, as well to monitor the performance of the duties and obligations, ensure appropriate internal controls on financial and accounting systems, and conduct investigations and other activities in connection with legal proceedings or in anticipation of potential proceedings.

West does not sell, rent, lease or transfer Personal Data about its employees to unaffiliated third parties except as otherwise provided in this Statement. West may, from time to time, disclose Personal Data about its employees to relevant third parties for its reasonable business and legal purposes. For example, West may seek to provide travel services or other benefits to its employees or it may be legally obligated by a government agency to disclose Personal Data. Recipients of such data may include affiliated corporate entities, including successor entities, agents, contractors involved with any payments or benefits, future employers who request a reference, proposed assignee or transferee of the business, as well as governmental, judicial or regulatory authorities in order to comply with legal or regulatory obligations or as authorized by the employee.

1.2 Sensitive Personal Data

Sensitive Personal Data are not disclosed to unaffiliated third parties or used for purposes other than those for which the data were initially collected without consent of the data subject or the presence of other circumstances requiring or justifying such use under applicable law. Sensitive Personal Data may be processed to meet West's legal responsibilities, for purposes of personnel management and administration, suitability for employment and to comply with equal opportunity legislation. For instance, in certain circumstances, it may be necessary for West to obtain a medical report from an employee's doctor in order to establish reasons for and likely duration of an absence, when an employee will be able to return to work, and whether the problem will recur, as well as, what, if any, treatment is being prescribed and whether an employee can carry out all the duties of the job.

Data subjects are given this notice of the processing performed on their Sensitive Personal Data and, where feasible and appropriate, opportunities to express their choices regarding Sensitive Personal Data. In particular, a choice is regularly offered where West seeks to use Sensitive Personal Data for a purpose that is incompatible with the original purposes for which the data were collected or subsequently authorized, or transferred to a third party that is not acting as an agent of West. West does not process Sensitive Personal Data in any manner not allowed by applicable law.

SECTION 2. DATA INTEGRITY & RETENTION

West endeavors to keep all Personal Data in its possession reasonably current and accurate. Employees are expected to keep West informed of any changes to their Personal Data such as a change in address or any other information affecting benefits or services provided by West. West strives to maintain Personal Data, including Sensitive Personal Data, for periods no more extensive than what is necessary for the purposes for which it was collected or for which it may be appropriately used, but it retains data when required to do so by law.

SECTION 3. ACCESS TO PERSONAL DATA

3.1 Employee access

Subject to applicable law and regulation, employees may inspect Personal Data in his or her personnel file, and if necessary request corrections to such data. Requests for such access must be made in writing to the employee's immediate manager. Human Resources shall keep a written record of such requests and will provide a response to such a request as soon as reasonably possible within the time frame required by law. Such response may include a determination Human Resources needs additional time to provide a response to the request. Upon receipt and verification of corrected Personal Data, Human Resources will ensure appropriate correction is made.

Access to Personal Data is not guaranteed, however, reasonable requests for access will be granted subject to West's rights and responsibilities and in accordance with applicable law and regulation.

3.2 No automated decision making without appropriate safeguards

West personnel are not subject to decisions concerning them which are based solely on automated processing of Personal Data unless appropriate human mechanisms are in place to safeguard against inaccurate or improper decisions.

SECTION 4. DATA SHARING

4.1 Service Providers

Personal Data regarding West employees may be shared with service providers who process data on behalf of West in order to supply West and its employees with the services necessary to manage the business including, for example, providing services to employees, former employees, and customers. For example, Personal Data may be shared with a vendor for purposes of executing West's payroll. Sensitive Personal Data, such as health information, may be shared with service providers for the purpose of administering employee benefits programs.

West requires all service providers, vendors and other processors of Personal Data to process such Personal Data under the direction of West and provide adequate protections for the Personal

Data entrusted to them by West, at least at the same level of privacy protection as required by these privacy principles. West will only transfer Personal Data to a non-agent third party where such transfer is consistent with the notice provided to the data subjects at the time the Personal Data were collected.

West may use or disclose employees' Personal Data if required to do so by law or in the good faith belief such action is necessary to adhere to any applicable law or comply with legal process served on or applicable to West, protect and defend the rights or property of West, or act to protect the personal safety of West employees or members of the public or otherwise aid law enforcement or protect national security. West may also disclose Personal Data or other data relating to personnel to anyone the data subject authorizes.

West may disclose Personal Data to third parties where necessary to comply with any legal obligation of West, in connection with actual or prospective legal proceedings against West and otherwise in connection with the establishment, investigation, exercise or defense of legal claims.

In the event of a sale, assignment, bankruptcy, liquidation or other transfer of all or substantially all of the stock, assets or business of West, Personal Data may be transferred to a relevant successor entity, subject to the applicable privacy statement. Any corporate successors to West may be provided with employee files during a corporate transaction including during any due diligence process for prospective transactions, provided the receiving party agrees to privacy and security conditions equivalent to those provided in this Statement.

4.2 Intra-West transfers

As a global corporation operating in several countries, West transfers Personal Data between offices of West across national borders for the purposes of international administration and operations or for any of the other purposes referred to in this Statement. Such intra-West transfers of Personal Data may result in the transfer of data between countries that have differing legal regimes for privacy protection and provide different levels of privacy protection. In particular, data are routinely transferred between the European Union and other countries around the world, some of which the European Union currently does not deem to have "adequate" privacy safeguards. One purpose of this Statement is to address this concern by ensuring the data transferred will be consistently treated with best practices and a high-level standard of protection regardless of the office location.

Personal Data are processed and transferred between the Company's offices pursuant to the data protection requirements of this Statement. Such transfers will take place on the basis of: (i) the consent of the data subject, (ii) the EU's standard contractual clauses for data transfers; (iii) being necessary for the performance of a contract between the data subject and the Company or the implementation of such pre-contractual measures taken in response to the data subjects request; (iv) being necessary for the conclusion or performance of a contract in the interest of the data subject between the Company and third parties; or (v) being necessary or legally required on important public interest grounds or for the establishment, exercise or defense of legal claims.

SECTION 5. MONITORING

West may monitor the activities of its personnel consistent with applicable law for certain purposes including compliance with regulatory practices, quality control, to prevent or detect crime, to investigate unauthorized use, or to determine whether communications are business or

personal communications. For instance, West may use security monitoring devices, such as remote cameras in lobbies of offices and key-cards to enter offices, when allowed by law.

West may also conduct background checks or other investigations of personnel in accordance with applicable law when West deems such information necessary to protect the Company or its customers.

West may provide its employees with technologies such as voice mail, mobile phones, mobile devices, computers, internet access, instant messaging, email, and fax machines, for carrying out the business of the Company. Except as may be required under applicable local law, personnel should not expect that any personal communication using Company resources is or will remain private regardless of the use of passwords. West monitors and otherwise accesses email, internet access or use, and other transmissions made using its technology resources for the purposes referred to above, consistent with applicable law. Deletion of documents, data or communications does not necessarily mean the items cannot still be monitored or retrieved and reviewed. Personal communications should be directed to home addresses, rather than the Company.

Personnel shall not be subject to electronic recording of the content of their direct telephone conversations, except as may be permitted under applicable law. West does not operate any electronic surveillance device or system, including but not limited to the recording of sound or voice or a closed circuit television system, or any combination thereof, for the purpose of recording or monitoring the activities of Personnel in areas designed for the health or personal comfort of Personnel or for safeguarding their possessions, such as rest rooms, locker rooms, or rest areas.

Employees are prohibited from sending or downloading defamatory, illegal or pornographic email, or other similar Internet content in accordance with company policies found on the West Human Resources Intranet page. Notwithstanding any other general principle, whenever West has reasonable grounds to believe any employee is engaged in conduct that violates the law, violates the legal rights of West or other employees, endangers the physical safety of any person, creates a hostile workplace environment, or is necessary to comply with applicable law, West may conduct monitoring without giving any further prior written notice. Any employee, device, or workplace monitoring, of whatever type, shall be conducted only when necessary, in a proportional and nondiscriminatory manner, using the least-restrictive means necessary to achieve the required purpose, and in accordance with applicable law.

SECTION 6. INFORMATION SECURITY

Information security is an important component of West's data protection obligations. West takes appropriate precautions to restrict access to Personal Data to only those West personnel with a need to know. West implements and maintains reasonable and appropriate measures to protect the Personal Data in its possession from loss, misuse, unauthorized access or inadvertent destruction. West also maintains physical, electronic and procedural safeguards in order to protect the data under its control. West's Information Security Policy Manual is available to West employees through the West Intranet home page.

West personnel are responsible for maintaining information security with respect to Personal Data and must take all appropriate precautions to protect against unauthorized access to West's computer networks and information systems, including protection of user-IDs and passwords.

All employees and each department must ensure all devices containing Personal Data are properly disposed of when taken out of service.

West evaluates and implements new information security technologies and practices on an ongoing basis and will, from time to time, communicate new or additional requirements to West employees.

Despite West's best efforts, security cannot be guaranteed against all threats. Should a breach of security occur, please immediately notify breach@west.com, as well as the Business Unit manager so West can investigate the breach and take appropriate steps under the circumstances, consistent with its legal obligations.

EFFECTIVE DATE

This statement is effective as of March 20, 2018 for all of West Corporation.