BIOMETRIC DATA POLICY - ASSOCIATES

Zurn Industries, LLC (the "Company") is committed to all employees being paid accurately and on-time. To accomplish this purpose, the Company has implemented a state of the art timekeeping system at certain facilities in order to collect hours worked by employees. The Company has partnered with a leading third-party vendor to provide technology to efficiently and easily collect and/or store data for this purpose.

Rather than solely punching a timecard, or scanning an ID badge, an employee will "log" into the system by entering their employee ID number followed by using finger scan technology. This technology does not actually collect or store fingerprints. Instead, the system measures certain biometric aspects of an employee's fingertip. Those fingerprint biometric data points are immediately converted through a proprietary software program to a unique mathematical representation of that data, which is encrypted and saved in a template. No optical image of a finger scan is kept. Each time an employee clocks in for work, a new finger scan will be provided and the template from that scan will be compared with the template assigned to the employee's personalized ID number to verify the identity of the employee.

The Company is also committed to protecting the health and well-being of its employees. Towards that goal, the Company is installing and deploying a personnel check-in temperature verification system at the entrance to certain facilities, which will measure the body temperature of associates entering the facilities. The temperature verification system can be set up and used to identify individuals through the use of face scan technology. The Company will not use this function of the system, and no identification of personnel will take place by way of scan technology. However, even though the Company will not access or use any data generated or resulting from the face scan capability of the temperature verification system, it is possible that certain data from the face scan function will be stored within the system.

The fingerprint biometric data points, or templates, and any face scan data created by the temperature verification system, are referred to as Biometric Data.

Employees of the Company will be required to consent as a condition of employment to the Company's (and its selected timekeeping and storage vendors') capture, collection and storage of Biometric Data from the finger scan technology for timekeeping purposes and from the temperature verification system. However, the Company will consider requests by employees for accommodation or exemption in whole or in part from the procedures set forth in this policy and/or the use by the Company of finger scan technology and biometric data for verification of employees' identities, or in connection with temperature verification. Prior to giving consent, employees should read this policy, which will be presented to employees upon employment and enrollment into the timekeeping system, and prior to the use of the temperature verification system, and which is also available at any time through Human Resources, including the Human Resources' web site and through the Company's website at www.zurn.com.

The Company understands that in today's world, people may be concerned about the security of their personal information. With this in mind, the Company has carefully selected vendors that share the Company's commitment to protecting confidential and sensitive information. The Company, and its vendors, will store, transmit, and protect from disclosure, all Biometric Data

obtained through the finger scan technology, or the temperature verification system, using the reasonable standard of care within the industry and in a manner that is the same or more protective than the manner in which the Company stores, transmits and protects any other confidential information.

During an employee's employment, the Biometric Data from the timekeeping system, which is stored by the vendor, is not accessible by any Company representative or by any in-company technology system. Due to the technology used, the data, or template, that is stored by the vendor is virtually impossible to restore to the original scan of the finger. Any Biometric Data generated by the temperature verification system will not be accessed or used for any purpose. Furthermore, the Company and its vendors will not sell, lease, trade, or otherwise profit from an employee's Biometric Data. The Company will not, and the Company's vendors have assured the Company that they will not, disclose or otherwise disseminate an employee's Biometric Data without an employee's consent unless required by any state or federal law, municipal ordinance, valid warrant, or valid subpoena.

Any employee Biometric Data collected will be retained by the Company and its vendors for one (1) year after the employee's last use of either system or one (1) year after termination, whichever is sooner, unless required by law to be maintained for a longer period – provided that the current timekeeping and temperature verification systems are maintained. The Company and its vendors will permanently destroy an employee's Biometric Data upon expiration of the aforesaid time periods.

This policy is intended to comply with all federal, state, and local laws, and will be interpreted and applied in order to comply with all applicable laws, including but not limited to the Illinois Biometric Information Privacy Act and Tex. Bus. & Com. Code Ann. Section 503.001. Any legal disputes, claims, controversies or disagreements arising out of or relating to this policy or the Company's procedure relating to an employee's Biometric Data ("Claim") shall be resolved by binding arbitration instead of the courts. All Claims may be brought only in the employee's individual capacity, and not as Plaintiff, claimant or class member in a class, collective or other representative or joint proceeding. Arbitration is the exclusive form for the resolution of such Claims, and both the Company and employees mutually waive their respective right to a trial before a judge or jury in federal or state court. The binding arbitration will be administered by the American Arbitration Association ("AAA") in accordance with its rules and procedures then in effect, and shall be confidential.

If any provision of this Biometric Data Policy or any part thereof contravenes any law, or if the operation of any provision hereof is determined by law or otherwise to be unenforceable, then such offending provision or part thereof shall be severed and the remaining provisions given full force and effect.

If you have any questions about this policy, including how the finger scan technology or the temperature verification system work, how the finger scan technology or temperature verification system is used, or how the timekeeping system interfaces with the payroll process, please contact your facility Human Resources Manager.

Informed Written Consent for the Collection, Storage, and Use of Biometric Data

Zurn Industries, LLC (the "Company"), as set forth in the Biometric Data Policy which has been provided, utilizes a timekeeping system that uses, in part, Biometric Data in the form of templates derived from employees' finger scans. At no point are employees' actual fingertip images stored, and the finger scans are completely discarded after the templates are created. The templates are then stored in a secure database and used to verify employee's identities upon arrival at the place of work. The Company also utilizes a temperature verification system, which will measure the body temperature of those entering the facilities. The temperature verification system can be set up and used to identify individuals through the use of face scan technology, although the Company will not use this function of the system, and no identification of personnel will take place by way of face scan technology. However, even though the Company will not access or use any data generated or resulting from the face scan capability of the temperature verification system, it is possible that certain data from the face scan function will be stored within the temperature verification system.

The fingerprint biometric data points, or templates, and any face scan data created by the temperature verification system, are referred to as Biometric Data.

Prior to participating in the Company's use of Biometric Data, please take notice of the following:

1. It is possible that the scan of your fingertips, and the templates derived therefrom, or data created from the temperature verification systems, may be subject to provisions of the Illinois Biometric Information Privacy Act and Tex. Bus. & Com. Code Ann. Section 503.001;

2. Your employment at the Company will involve the scan of your fingertip and storage of the templates derived therefrom, and the verification of your temperature, which may involve a scan of your face;

3. The templates derived from your finger scans or data generated from any face scans will be collected, stored, and used for the duration of your employment, but in no event longer than one (1) year after your last interaction with a system or one (1) year after your termination of employment with the Company unless required by law to be maintained for a longer period; and

4. The templates derived from your finger scans will be collected, stored, and used for the specific purpose of verifying your identity.

Having read the above and the Biometric Data Policy, I agree to the following:

1. The templates or Biometric Data derived from my finger scans or face scans may be collected, used, and stored for the duration of my employment, but in no event longer than one (1) year after my last interaction with a system or one (1) year after my termination of employment with the Company unless required by law to be maintained for a longer period;

2. The templates or Biometric Data derived from my finger scans will be collected, used, and stored for the specific purpose of verifying my identity; and

3. By signing this document, I am providing the Company with a legally effective written release (i.e., informed written consent) to collect, store, and use the templates or Biometric Data derived from my finger scans or face scans.

_____ _____

EMPLOYEE'S SIGNATURE DATE

_____

EMPLOYEE'S NAME (Please Print)

BIOMETRIC DATA POLICY - VISITORS

Zurn Industries, LLC (the "Company") is committed to protecting the health and well-being of its employees and visitors. Towards that goal, the Company is installing and deploying a visitor check-in temperature verification system and a denied party screening system at the entrance to certain facilities. The temperature verification system will measure body temperature and the denied party screening system will check the visitor's name against a denied party's list. These systems can be set up and used to identify individuals through the use of face scan technology. The Company will not use this function of the systems, and no identification of persons will take place by way of face scan technology. However, even though the Company will not access or use any data generated or resulting from the face scan capability of the systems, it is possible that certain data from the face scan function will be stored within the systems.

Any face scan data created by the systems, are referred to as Biometric Data.

Visitors of the Company will be required to consent as a condition to entering a Company facility to the capture, collection and storage of Biometric Data from the systems. Prior to giving consent, visitors should read this policy, which will be presented to visitors as part of their check-in process, and which is also available through the Company's website at www.Zurn.com.

The Company understands that in today's world, people may be concerned about the security of their personal information. The Company will store, transmit, and protect from disclosure, all Biometric Data obtained through the systems, using the reasonable standard of care within the industry and in a manner that is the same or more protective than the manner in which the Company stores, transmits and protects any other confidential information.

Any Biometric Data generated by the systems will not be accessed or used for any purpose. Furthermore, the Company will not sell, lease, trade, or otherwise profit from a visitor's Biometric Data. The Company will not disclose or otherwise disseminate a visitor's Biometric Data without consent unless required by any state or federal law, municipal ordinance, valid warrant, or valid subpoena.

Any visitor Biometric Data collected will be retained by the Company for one (1) year after the visitor's last use of the system, unless required by law to be maintained for a longer period – provided that the current temperature verification and denied party screening systems are maintained. The visitor's Biometric Data shall be deleted upon expiration of the aforesaid time period.

This policy is intended to comply with all federal, state, and local laws, and will be interpreted and applied in order to comply with all applicable laws, including but not limited to the Illinois Biometric Information Privacy Act and Tex. Bus. & Com. Code Ann. Section 503.001. Any legal disputes, claims, controversies or disagreements arising out of or relating to this Zurn Biometric Data Policy or the Company's procedure relating to Biometric Data ("Claim") shall be resolved by binding arbitration instead of the courts. All Claims may be brought only in a visitor's individual capacity, and not as Plaintiff, claimant or class member in a class, collective or other representative or joint proceeding. Arbitration is the exclusive form for the resolution of such

Claims, and both the Company and the visitor mutually waive their respective right to a trial before a judge or jury in federal or state court. The binding arbitration will be administered by the American Arbitration Association ("AAA") in accordance with its rules and procedures then in effect, and shall be confidential.

If any provision of this Biometric Data Policy or any part thereof contravenes any law, or if the operation of any provision hereof is determined by law or otherwise to be unenforceable, then such offending provision or part thereof shall be severed and the remaining provisions given full force and effect.

If you have any questions about this policy, including how these systems works or are used, please contact your host.

Informed Written Consent for the Collection, Storage, and Use of Biometric Data

Zurn Industries, LLC (the "Company"), as set forth in the Biometric Data Policy-Visitors which has been provided, utilizes a temperature verification system and a denied party screening system. The temperature verification system will measure body temperature and the denied party screening system will check the visitor's name against a denied party's list. The systems can be set up and used to identify individuals through the use of face scan technology, although the Company will not use this function of the systems, and no identification of visitors will take place by way of face scan technology. However, even though the Company will not access or use any data generated or resulting from the face scan capability of the systems, it is possible that certain data from the face scan function will be stored within the systems.

Any face scan data created by the systems, are referred to as Biometric Data.

Prior to entering the Company's facility, please take notice of the following:

4. It is possible that data created from the systems may be subject to provisions of the Illinois Biometric Information Privacy Act and Tex. Bus. & Com. Code Ann. Section 503.001;

5. Your entrance to a Company facility may involve the verification of your temperature and a check of your name against a denied parties list, which may involve a scan of your face; and

6. The data generated from any face scans will be collected and stored no longer than one (1) year after your last interaction with the systems unless required by law to be maintained for a longer period, .

Having read the above and the Biometric Data Policy, I agree to the following:

7. The Biometric Data derived from my face scans may be collected, used, and stored no longer than one (1) year after my last interaction with the Company and the systems unless required by law to be maintained for a longer period; and

8. By signing this document, I am providing the Company with a legally effective written release (i.e., informed written consent) to collect, store, and use the Biometric Data derived from my face scans.

_____ _____

VISITOR'S SIGNATURE DATE

_____

VISITOR'S NAME (Please Print)