workforce SOFTWARE | MAKING WORK EASY

BIOMETRIC SECURITY STANDARD

Version:	1.0
Date of version:	March 30, 2018
Created by:	Mike Muha, CISO & CPO
Approved by:	Tammy Pidgeon, Legal
Owner:	Mike Muha, CISO & CPO
Confidentiality level:	Public

Change History

Date	Version	Created By	Description of Change
March 30, 2018	1.0	Michael J. Muha	Original draft

Contents

1. About this Document

1.1 Intended Audience

This document is intended for all individuals involved in determining the business need for the collection of Biometric Data, as well as individuals involved in implementation and support for biometric devices and Biometric Data.

1.2 Purpose

To define the policy and procedures for collection, use, safeguarding, storage, retention, and destruction of Biometric Data processed by WorkForce Software while acting as a Data Controller or as a Data Processor. This document also describes recommended, and in certain cases, required complementary controls for customers using biometric data collection devices.

1.3 Related Documents

- ISO/IEC 27001 standard, clauses A.18.1.4
- General Data Protection Regulation, Articles 5, 6, 7, 9
- Illinois Biometric Information Privacy Act ("IBIPA")
- WorkForce Software Cryptographic Standards

2. Scope

This standard applies to any systems, processes, and people used to process and manage Biometric Data. The scope includes the use of Biometric Data within WorkForce Software and makes recommendations for, and, in certain cases, requirements of customers who buy data collection devices from WorkForce Software that process biometric data. Nothing in this document is intended to relieve any customer of any obligations contained in its contract with WorkForce Software or otherwise required by applicable law. To the extent any provisions of this document conflict with a customer's contract, such contract shall control.

3. Responsibilities

The Chief Information Security Officer and Chief Privacy Officer is responsible for maintaining this policy.

WorkForce Software staff are responsible for adhering to this standard.

WorkForce Software reserves the right to amend this Biometric Security Standard at any time.

4. Standard as a Data Controller

This section describes the standards around WorkForce Software acting as a Data Controller and collecting, storing and processing Biometric Data for its own purposes. (See "6. Complementary controls for customers" for recommendations, and, in certain circumstances, requirements for customers that collect biometric data).

4.1 The collection of biometric data is prohibited except for specific circumstances

The collection of biometric data is prohibited unless the data subject has given explicit consent for the processing of their biometric data for one or more specified purposes.

4.2 Conduct a Data Protection Impact Assessment prior to the collection

Privacy impact assessments should be conducted before biometric data is collected in order to determine whether the collection of biometric data is necessary and, if so, to what extent. The EU General Data Protection Regulation classifies biometric data as sensitive data that requires a privacy impact assessments to be carried out in certain instances of processing of biometric data.

4.3 Only collect the biometric data you really need

In line with the general data collection limitation principle, the collection of biometric data must be:

- for a lawful purpose related directly to the collecting organisation's functions and activities; and
- necessary and not excessive for achieving such purpose.

In other words, because of the sensitivity of biometric data, its collection requires a strong justification. If an intended (valid) purpose can be achieved by collecting less sensitive biometric data or other data, then only that data must be collected. Biometric systems should not be adopted because they are the most convenient or cost-effective option, they must only be implemented if they are necessary and there is no less privacy-invasive way of achieving an intended outcome.

4.4 Consent to use biometric data must be explicit

The data subject must give consent, and that consent must be explicit and written, before the collection of biometric data. A data subject also has the right to withdraw consent at any time. A consent statement should be tailored to fit the type of biometric data collected.

4.5 Provide notice. Offer choice.

Prior to the collection of biometric data, the relevant individuals must be informed comprehensively about the impact of the intended collection and use of biometric data and they should be offered the choice of less privacy-intrusive alternatives. Their free and express consent must be obtained prior to the collection. Covert collection of biometric data violates this rule.

The notice must include the following:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative (i.e., WorkForce Software);
2. the contact details of the data protection officer or privacy officer;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. the recipients or categories of recipients of the personal data, if any;

5. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of a legal means of transfer (e.g., GDPR Articles 44-50);
6. the retention period of the data or the criteria used to determine the period[1];
7. the existence of the rights of rectification (fix or amend data), erasure, restrict processing, or object to processing;
8. the right to lodge a complaint with a supervisory authority (EU), binding arbitration, or other privacy authority;
9. if the data will be used for automated decision-making; and
10. the right to have a copy of their data.

4.6 Apply Risk Minimization Techniques

Where possible, risk minimization techniques should be applied (or must be applied if and when required by applicable law), including that:

- biometric templates (which consist of summary information only) rather than raw data should be stored to minimize the amount of data stored;
- generally, verification biometric systems should be favoured over identification systems as they collect less biometric features;
- if possible, biometric information should be stored locally (such as on smart cards or security tokens) rather than in central databases as it gives individuals more control over their biometric information and reduces the risk of data loss or inappropriate cross-linking of data across systems.
- WorkForce Software will protect and store biometric data in accordance with applicable standards, regulations, and laws.
- WorkForce Software will store, transmit, and protect biometric data using the same standard of care and security controls it provides for Personal Information in its possession.
- Protect confidentiality and integrity of databases containing biometric data
- An individual's biometric data will not be collected or otherwise obtained without prior written consent of the individual. WorkForce Software will inform the individual of the reason his or her biometric information is being collected and the length of time the data will be stored.[2] A consent statement should be tailored to fit the type of biometric data collected.

4.7 Disclosure

- WorkForce Software will not sell, lease, trade, or otherwise profit from an individual's biometric data.

---

[1] IBIPA, if applicable, requires that this period be *the shorter of* the satisfaction of the reason for the collection or three (3) years.
[2] IBIPA, if applicable, requires that this period be *the shorter of* the satisfaction of the reason for the collection or three (3) years.

- Biometric data will not be disclosed by WorkForce Software unless (a) consent is obtained, (b) disclosure is necessary to complete a financial transaction requested or authorized by the subject, (c) disclosure is required by law, or (d) disclosure is required by subpoena.

4.8 Data retention and destruction

- Biometric data will be stored using a reasonable standard of care and in a manner that is the same or exceeds the standards used to protect other confidential information held by WorkForce Software.
- A data retention policy must be defined and documented[3].
- WorkForce Software will destroy biometric data when the initial purpose for obtaining or collecting such data has been fulfilled.

5. Standard as a Data Processor

This section describes the standards around WorkForce Software acting as a Data Processor and collecting, storing and processing biometric data on behalf of a Data Controller (e.g., customer).

5.1 Contracts should require compliance with regulations and indemnify WFS

WFS should include terms in its sale contracts and subscription agreements requiring the purchaser/subscriber to comply with regulations around the collection of biometric data and to indemnify WFS.

WFS's contracts and subscription agreements should include provisions that require the purchasers and subscribers to adhere to all applicable biometric regulations (e.g., the Illinois Biometric Information Privacy Act). These provisions should specify that the purchaser/subscriber shall, among other things,

1. provide the necessary disclosures to and obtain the requisite consents and releases from the employees that use WFS's systems (such releases should include both the employer and WFS);
2. strictly adhere to the IBIPA's requirements for distribution or other disclosure, storage, protection, and destruction of biometric information, if subject to the IBIPA; and
3. indemnify WFS for any damages it incurs for the purchaser's/subscriber's failure to comply with regulations.

5.2 Avoid accidental collection of biometric data

To eliminate risk of falling within the requirements of various states' fingerprint laws, WFS should avoid collecting any actual fingerprints and should make reasonable efforts to have its customers "wipe" all WFS equipment of any stored fingerprints before returning any equipment to WFS.

[3] The IBIPA Sec. 15 specifically requires a biometric policy and that biometric data be destroyed when the initial purpose for using the data has been satisfied or within three (3) years of the individual's last interaction with the organization.

5.3 Conduct a Data Protection Impact Assessment prior to the collection

Privacy impact assessments should be conducted before biometric data is collected, stored, or processed to determine whether the collection of biometric data is necessary and, if so, to what extent. Note that the EU General Data Protection Regulation classifies biometric data as a special category of data that requires a privacy impact assessment to be carried out in certain instances of processing of biometric data.

5.4 Only collect the biometric data you really need

In line with the general data collection limitation principle, the collection of biometric data must be:

- for a lawful purpose related directly to the collecting organisation's functions and activities; and
- necessary and not excessive for achieving such purpose.

In other words, because of the sensitivity of biometric data, its collection requires a strong justification. If an intended (valid) purpose can be achieved by collecting less sensitive biometric data or other data, then only that data must be collected. Biometric systems should not be adopted because they are the most convenient or cost-effective option, they must only be implemented if they are necessary and there is no less privacy-invasive way of achieving an intended outcome.

5.5 Consent to use biometric data must be explicit

If required by applicable law, the data subject must give consent, and that consent must be explicit and written, before the collection of biometric data. A data subject also has the right to withdraw consent at any time. A consent statement should be tailored to fit the type of biometric data collected. The Data Controller, not WorkForce Software, is responsible for obtaining consent.

5.6 Apply Risk Minimization Techniques

Where possible, risk minimization techniques should be applied (or shall be applied if required by applicable law), including:

- biometric templates (which consist of summary information only) rather than raw data should be stored to minimize the amount of data stored;
- generally, verification biometric systems should be favoured over identification systems as they collect less biometric features;
- if possible, biometric information should be stored locally (such as on smart cards or security tokens) rather than in central databases as it gives individuals more control over their biometric information and reduces the risk of data loss or inappropriate cross-linking of data across systems.
- WorkForce Software will protect and store biometric data in accordance with applicable standards, regulations, and laws.
- WorkForce Software will store, transmit, and protect biometric data using the same standard of care and security controls it provides for Personal Information in its possession.
- Protect confidentiality and integrity of databases containing biometric data

- An individual's biometric data will not be collected or otherwise obtained without prior written consent of the individual. WorkForce Software will inform the individual of the reason his or her biometric information is being collected and the length of time the data will be stored. A consent statement should be tailored to fit the type of biometric data collected.

5.7 Disclosure

- Biometric data will not be disclosed by WorkForce Software unless (a) consent is obtained from the Data Controller (who in turn, may be required to gain consent from the Data Subject), (b) disclosure is necessary to complete a financial transaction requested or authorized by the Data Controller, (c) disclosure is required by law, or (d) disclosure is required by subpoena.

5.8 Data retention and destruction

- Biometric data will be stored using a reasonable standard of care and in a manner that is the same or exceeds the standards used to protect other confidential information held by WorkForce Software.
- A data retention policy must be defined and documented[4].
- WorkForce Software will destroy biometric data when the initial purpose for obtaining or collecting such data has been fulfilled.

6. Complementary controls for customers

This section makes recommendation of complementary controllers for customers who purchase from WorkForce Software any hardware or services that process or store biometric data. Certain of these recommendations, however, are actual requirements provided by the Illinois Biometric Information Privacy Act (indicated by the notation (IBIPA)) that may apply to certain customers. The customer is responsible for knowing and complying with any applicable laws that govern its collection and use of biometric data.

6.1 The collection of biometric data is prohibited except for specific circumstances

The customer should evaluate regulations and laws around the collection of biometric data. Generally, the collection of biometric data is prohibited except for these specific circumstances:

- If the data subject has given explicit consent for the processing of their biometric data for one or more specified purposes.
- If processing of biometric information is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller (WorkForce Software) or of the data subject in the field of employment and social security and social protection law.
- If processing is necessary to protect the vital interests of the data subject and he/she is incapable of giving consent.

[4] The IBIPA Sec. 15 specifically requires a biometric policy and that biometric data be destroyed when the initial purpose for using the data has been satisfied or within three years of the individual's last interaction with the organization.

- If processing is necessary for the establishment, exercise or defence of legal claims.
- If processing is necessary for reasons of public interest in the area of public health.

6.2 Conduct a Data Protection Impact Assessment prior to the collection

Customers should conduct a privacy impact assessment before biometric data is collected in order to determine whether the collection of biometric data is necessary and, if so, to what extent. The EU General Data Protection Regulation classifies biometric data as sensitive data that requires a privacy impact assessments to be carried out in certain instances of processing of biometric data.

6.3 Only collect the biometric data you really need

In line with the general data collection limitation principle, the collection of biometric data must be:

- for a lawful purpose related directly to the collecting organisation's functions and activities; and
- necessary and not excessive for achieving such purpose.

In other words, because of the sensitivity of biometric data, its collection requires a strong justification. If an intended (valid) purpose can be achieved by collecting less sensitive biometric data or other data, then only that data must be collected. Biometric systems should not be adopted because they are the most convenient or cost-effective option, they must only be implemented if they are necessary and there is no less privacy-invasive way of achieving an intended outcome.

6.4 Consent to use biometric data must be explicit

The data subject must give consent, and that consent must be explicit and written, before the collection of biometric data. (IBIPA) A data subject also has the right to withdraw consent at any time. A consent statement should be tailored to fit the type of biometric data collected. (IBIPA)

6.5 Provide notice. Offer choice.

Prior to the collection of biometric data, the relevant individuals must be informed comprehensively about the impact of the intended collection and use of biometric data and they should be offered the choice of less privacy-intrusive alternatives. Their free and express consent must be obtained prior to the collection. The (in practice frequently used) covert collection of biometric data violates this rule.

The notice must include the following:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative (i.e., WorkForce Software);
2. the contact details of the data protection officer or privacy officer;
3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing (IBIPA);
4. the recipients or categories of recipients of the personal data, if any;
5. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of a legal means of transfer (e.g., GDPR Articles 44-50);

6. the retention period of the data or the criteria used to determine the period (IBIPA);
7. the existence of the rights of rectification (fix or amend data), erasure, restrict processing, or object to processing;
8. the right to lodge a complaint with a supervisory authority (EU), binding arbitration, or other privacy authority;
9. If the data will be used for automated decision-making;
10. The right to have a copy of their data.

6.6 Apply Risk Minimization Techniques

Where possible, risk minimization techniques should be applied, including that:

- biometric templates (which consist of summary information only) rather than raw data should be stored to minimize the amount of data stored;
- generally, verification biometric systems should be favoured over identification systems as they collect less biometric features;
- if possible, biometric information should be stored locally (such as on smart cards or security tokens) rather than in central databases as it gives individuals more control over their biometric information and reduces the risk of data loss or inappropriate cross-linking of data across systems.
- The customer should protect and store biometric data in accordance with applicable standards, regulations, and laws (IBIPA).
- The customer should store, transmit, and protect biometric data using the same standard of care and security controls it provides for Personal Information in its possession (IBIPA).
- Protect confidentiality and integrity of databases containing biometric data
- An individual's biometric data will not be collected or otherwise obtained without prior written consent of the individual. (IBIPA) The customer should inform the individual of the reason his or her biometric information is being collected and the length of time the data will be stored. (IBIPA) A consent statement should be tailored to fit the type of biometric data collected.

6.7 Data retention and destruction

- Biometric data should be stored using a reasonable standard of care and in a manner that is the same or exceeds the standards used to protect other confidential information held by customer. (IBIPA)
- A data retention policy should be defined and documented. (IBIPA)
- The customer should destroy biometric data when the initial purpose for obtaining or collecting such data has been fulfilled. (IBIPA)

7. Enforcement

Any WorkForce Software staff found to have violated this standard and/or associated policies may be subject to disciplinary action, up to and including termination of employment.

8. Definitions and Acronyms

This section provides definitions for all acronyms and terms introduced in, unique, or important to this document.

Term	Definition
Biometrics	Automated method of identifying or verifying the identity of a living person based on unique biological or behavioral characteristics.
Biometric Data	Biometric Data means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (i.e. fingerprints). Biometric data can include fingerprints, voiceprints, facial shape, or scan of hand or face geometry.
Data Controller	The natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	The natural or legal person or other body which processes personal data on behalf of the controller.
Data Subject	An identified or identifiable natural person.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Third-Party	A natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.