workforce SOFTWARE | MAKING WORK EASY

ISO 27001:2013

CERTIFICATE & STATEMENT OF APPLICABILITY

Version:	4.0
Date of version:	August 30, 2019
Created by:	Michael. J. Muha
Approved by:	Michael J. Muha Chief Information Security & Privacy Officer
Owner:	Michael J. Muha Chief Information Security & Privacy Officer
Confidentiality level:	Public

Change History

Date	Version	Created By	Description of Change
September 13, 2016	1.0	Michael J. Muha, Director of Security & Privacy	Original document
August 7, 2017	2.0	Michael J. Muha, Chief Information Security & Privacy Officer	Added new certificate, updated format with new logo
August 8, 2018	3.0	Michael J. Muha Chief Information Security & Privacy Officer	Updated certificate
August 30, 2019	4.0	Michael J. Muha Chief Information Security & Privacy Officer	Updated certificate that includes all of WorkForce Suite, including the Forecasting & Scheduling product

schellman
Quality, above all.

CERTIFICATE OF REGISTRATION

Information Security Management System - ISO/IEC 27001:2013

The Certification Body of Schellman & Company, LLC hereby certifies that the following organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013

WorkForce Software, LLC

for the following scope of registration

The scope of the ISO 27001:2013 certification is limited to the information security management system (ISMS) supporting the WorkForce Software United States (US), European Union (EU), and Canada Software as a Service (SaaS) environments as it relates to the storing and/or processing of data classified as 'Customer Confidential' in the following WorkForce Suite modules: Time and Attendance, Forecasting and Scheduling, Advanced Scheduler, Absence Compliance Tracker, WorkForce Analytics, and Fatigue Management, and in accordance with the Statement of Applicability Version 1.6, dated July 31, 2019.

which includes the following in-scope location(s) on page 2 of 2

Certificate Number: **1736251-4**

ISO 27001 CERTIFIED by schellman

ANAB ACCREDITED MANAGEMENT SYSTEMS CERTIFICATION BODY

UKAS MANAGEMENT SYSTEMS 8685

Authorized by:

Christopher L. Schellman
CEO, Schellman & Company, LLC
4010 W Boy Scout Blvd., Suite 600
Tampa, Florida 33607, United States
www.schellman.com

Issue Date	Original Registration Date	Expiration Date	Certificate Version
August 30, 2019	September 13, 2016	September 11, 2022	Version 4

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO/IEC 27001:2013 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance audits by Schellman & Company, LLC
3. ISO/IEC 27001:2013 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. As such, this certification should not be construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. Schellman & Company, LLC expressly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of Schellman & Company, LLC and is bound by the conditions of contract. The authenticity of this certificate can be validated by contacting Schellman & Company, LLC

Certificate Number: **1736251-4**

In-Scope Location(s)

Location	Function / Role
38705 Seven Mile Road Livonia, Michigan 48152 United States	Main Location of the ISMS, Human Resources (HR), Information Technology (IT), Legal, Compliance, Operations, Sales, and Marketing
Precedent Drive, Rooksley Milton Keynes Buckinghamshire, MK13 8PP United Kingdom	IT, Operations
24700 Northwestern Highway, Suite 700 Southfield, Michigan 48075 United States	Data Center
12655 Edison Drive Alpharetta, Georgia 30005 United States	Data Center
7365 Lindell Road Las Vegas, Nevada 89139 United States	Data Center
Duivendrechtsekade 80A Amsterdam, 1096 AH Netherlands	Data Center
Gutleutstrasse 310 Frankfurt, 60327 Germany	Data Center
550 Cochrane Drive Markham, Ontario L3R8E2 Canada	Data Center
34 Highland Park Way NE Airdrie, Alberta T4A0R1 Canada	Data Center

Introduction

This document holds the Statement of Applicability (SOA) to support the certification for the ISO27001:2013 standard for information security. The objective of this document is to identify and implement the relevant control measures necessary to mitigate the possibility and impact of threats that WorkForce Software has recognized during the risk analysis, service reviews and audits.

The identified control measures are based on the ISO27001: Annex A Reference control objectives and controls.

The applicability is represented for each control measure.

If a control measure is not applicable an explanation is given.

Management Statement

The Management of WorkForce Software declares the measures specified in this Statement of Applicability, which were confirmed in relation to the outcome of the risk analysis, and accepts the remaining risks of any measures taken.

Scope

The scope of the ISO 27001 Information Security Management System at WorkForce Software focuses on the people, information, software, hardware, telecommunications, and facilities specific to the WorkForce Software United States (US), Canada, and European Union (EU) SaaS environments as it relates to the storing and/or processing of data classified as ‘Customer Confidential’.

Statement of Applicability

ID	Controls according to ISO/IEC 27001	Applicability
A.5	**INFORMATION SECURITY POLICIES**	
A.5.1	Management direction for information security	
A.5.1.1	Policies for information security	Yes
A.5.1.2	Review of the policies for information security	Yes
A.6	**ORGANIZATION OF INFORMATION SECURITY**	
A.6.1	Internal organization	
A.6.1.1	Information security roles and responsibilities	Yes
A.6.1.2	Segregation of duties	Yes
A.6.1.3	Contact with authorities	Yes
A.6.1.4	Contact with special interest groups	Yes
A.6.1.5	Information security in project management	Yes
A.6.2	Mobile devices and teleworking	
A.6.2.1	Mobile device policy	Yes
A.6.2.2	Teleworking	Yes
A.7	**HUMAN RESOURCE SECURITY**	
A.7.1	Prior to employment	
A.7.1.1	Screening	Yes
A.7.1.2	Terms and conditions of employment	Yes
A.7.2	During employment	
A.7.2.1	Management responsibilities	Yes
A.7.2.2	Information security awareness, education and training	Yes
A.7.2.3	Disciplinary process	Yes
A.7.3	Termination and change of employment	
A.7.3.1	Termination or change of employment responsibilities	Yes
A.8	**ASSET MANAGEMENT**	
A.8.1	Responsibility for assets	
A.8.1.1	Inventory of assets	Yes
A.8.1.2	Ownership of assets	Yes
A.8.1.3	Acceptable use of assets	Yes
A.8.1.4	Return of assets	Yes
A.8.2	Information classification	
A.8.2.1	Classification of information	Yes
A.8.2.2	Labeling of information	Yes
A.8.2.3	Handling of assets	Yes

ID	Controls according to ISO/IEC 27001	Applicability
A.8.3	Media handling	
A.8.3.1	Management of removable media	Yes
A.8.3.2	Disposal of media	Yes
A.8.3.3	Physical media transfer	Yes
A.9	**ACCESS CONTROL**	
A.9.1	Business requirements of access control	
A.9.1.1	Access control policy	Yes
A.9.1.2	Access to networks and network services	Yes
A.9.2	User access management	
A.9.2.1	User registration and de-registration	Yes
A.9.2.2	User access provisioning	Yes
A.9.2.3	Management of privileged access rights	Yes
A.9.2.4	Management of secret authentication information of users	Yes
A.9.2.5	Review of user access rights	Yes
A.9.2.6	Removal or adjustment of access rights	Yes
A.9.3	User responsibilities	
A.9.3.1	Use of secret authentication information	Yes
A.9.4	System and application access control	
A.9.4.1	Information access restriction	Yes
A.9.4.2	Secure log-on procedures	Yes
A.9.4.3	Password management system	Yes
A.9.4.4	Use of privileged utility programs	Yes
A.9.4.5	Access control to program source code	Yes
A.10	**CRYPTOGRAPHY**	
A.10.1	Cryptographic controls	
A.10.1.1	Policy on the use of cryptographic controls	Yes
A.10.1.2	Key management	Yes
A.11	**PHYSICAL AND ENVIRONMENTAL SECURITY**	
A.11.1	Secure areas	
A.11.1.1	Physical security Perimeter – SaaS US	Yes
A.11.1.1	Physical security Perimeter – SaaS EU	Yes
A.11.1.1	Physical security Perimeter – SaaS Canada	Yes
A.11.1.1	Physical security Perimeter – Corporate Headquarters	Yes
A.11.1.2	Physical entry controls – SaaS US	Yes
A.11.1.2	Physical entry controls – SaaS EU	Yes
A.11.1.2	Physical entry controls – SaaS Canada	Yes

ID	Controls according to ISO/IEC 27001	Applicability
A.11.1.2	Physical entry controls – Corporate Headquarters	Yes
A.11.1.3	Securing offices, rooms and facilities – SaaS US	Yes
A.11.1.3	Securing offices, rooms and facilities – SaaS EU	Yes
A.11.1.3	Securing offices, rooms and facilities – SaaS Canada	Yes
A.11.1.3	Securing offices, rooms and facilities – Corporate Headquarters	Yes
A.11.1.4	Protecting against external and environmental threats – SaaS US	Yes
A.11.1.4	Protecting against external and environmental threats – SaaS EU	Yes
A.11.1.4	Protecting against external and environmental threats – SaaS Canada	Yes
A.11.1.5	Working in secure areas	Yes
A.11.1.6	Delivery and loading areas – SaaS US	Yes
A.11.1.6	Delivery and loading areas – SaaS EU	Yes
A.11.1.6	Delivery and loading areas – Canada	Yes
A.11.1.6	Delivery and loading areas – Corporate	Yes
A.11.2	Equipment	
A.11.2.1	Equipment siting and protection – SaaS US	Yes
A.11.2.1	Equipment siting and protection – SaaS EU	Yes
A.11.2.1	Equipment siting and protection – SaaS Canada	Yes
A.11.2.2	Supporting utilities – SaaS US	Yes
A.11.2.2	Supporting utilities – SaaS EU	Yes
A.11.2.2	Supporting utilities – SaaS Canada	Yes
A.11.2.3	Cabling security – SaaS US	Yes
A.11.2.3	Cabling security – SaaS EU	Yes
A.11.2.3	Cabling security – SaaS Canada	Yes
A.11.2.4	Equipment maintenance – SaaS US	Yes
A.11.2.4	Equipment maintenance – SaaS EU	Yes
A.11.2.4	Equipment maintenance – SaaS Canada	Yes
A.11.2.5	Removal of assets – SaaS US	Yes
A.11.2.5	Removal of assets – SaaS EU	Yes
A.11.2.5	Removal of assets – SaaS Canada	Yes
A.11.2.6	Security of equipment and assets off-premises – SaaS US	Yes
A.11.2.6	Security of equipment and assets off-premises – SaaS EU	Yes
A.11.2.6	Security of equipment and assets off-premises – SaaS Canada	Yes
A.11.2.7	Secure disposal or reuse of equipment	Yes
A.11.2.8	Unattended user equipment	Yes
A.11.2.9	Clear desk and clear screen policy	Yes

ID	Controls according to ISO/IEC 27001	Applicability
A.12	**OPERATIONS SECURITY**	
A.12.1	Operational procedures and responsibilities	
A.12.1.1	Documented operating procedures	Yes
A.12.1.2	Change management	Yes
A.12.1.3	Capacity management	Yes
A.12.1.4	Separation of development, testing and operational environments	Yes
A.12.2	Protection from malware	
A.12.2.1	Controls against malware	Yes
A.12.3	Backup	
A.12.3.1	Information backup	Yes
A.12.4	Logging and monitoring	
A.12.4.1	Event logging	Yes
A.12.4.2	Protection of log information	Yes
A.12.4.3	Administrator and operator logs	Yes
A.12.4.4	Clock synchronization	Yes
A.12.5	Control of operational software	
A.12.5.1	Installation of software on operational systems	Yes
A.12.6	Technical vulnerability management	
A.12.6.1	Management of technical vulnerabilities	Yes
A.12.6.2	Restrictions on software installation	Yes
A.12.7	Information systems audit considerations	
A.12.7.1	Information systems audit controls	Yes
A.13	**COMMUNICATIONS SECURITY**	
A.13.1	Network security management	
A.13.1.1	Network controls – SaaS US	Yes
A.13.1.1	Network controls – SaaS EU	Yes
A.13.1.1	Network controls – SaaS Canada	Yes
A.13.1.2	Security of network Services – SaaS US	Yes
A.13.1.2	Security of network Services – SaaS EU	Yes
A.13.1.2	Security of network Services – SaaS Canada	Yes
A.13.1.3	Segregation in networks	Yes
A.13.2	Information transfer	
A.13.2.1	Information transfer policies and procedures	Yes
A.13.2.2	Agreements on information transfer	Yes
A.13.2.3	Electronic messaging	Yes
A.13.2.4	Confidentiality or nondisclosure agreements	Yes

ID	Controls according to ISO/IEC 27001	Applicability
A.14	**SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**	
A.14.1	Security requirements of information systems	
A.14.1.1	Information security requirements analysis and specification	Yes
A.14.1.2	Securing application services on public networks	Yes
A.14.1.3	Protecting application services transactions	Yes
A.14.2	Security in development and support processes	
A.14.2.1	Secure development policy	Yes
A.14.2.2	System change control procedures	Yes
A.14.2.3	Technical review of applications after operating platform changes	Yes
A.14.2.4	Restrictions on changes to software packages	Yes
A.14.2.5	Secure system engineering principles	Yes
A.14.2.6	Secure development environment	Yes
A.14.2.7	Outsourced development	Yes
A.14.2.8	System security testing	Yes
A.14.2.9	System acceptance testing	Yes
A.14.3	Test data	
A.14.3.1	Protection of test data	Yes
A.15	**SUPPLIER RELATIONSHIPS**	
A.15.1	Information security in supplier relationships	
A.15.1.1	Information security policy for supplier relationships	Yes
A.15.1.2	Addressing security within supplier agreements	Yes
A.15.1.3	Information and communication technology supply chain	Yes
A.15.2	Supplier service delivery management	
A.15.2.1	Monitoring and review of supplier services	Yes
A.15.2.2	Managing changes to supplier services	Yes
A.16	**INFORMATION SECURITY INCIDENT MANAGEMENT**	
A.16.1	Management of information security incidents and improvements	
A.16.1.1	Responsibilities and procedures	Yes
A.16.1.2	Reporting information security events	Yes
A.16.1.3	Reporting information security weaknesses	Yes
A.16.1.4	Assessment of and decision on information security events	Yes
A.16.1.5	Response to information security incidents	Yes
A.16.1.6	Learning from information security incidents	Yes
A.16.1.7	Collection of evidence	Yes

ID	Controls according to ISO/IEC 27001	Applicability
A.17	**INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**	
A.17.1	Information security continuity	
A.17.1.1	Planning information security continuity	Yes
A.17.1.2	Implementing information security continuity	Yes
A.17.1.3	Verify, review and evaluate information security continuity	Yes
A.17.2	Redundancies	
A.17.2.1	Availability of information processing facilities	Yes
A.18	**COMPLIANCE**	
A.18.1	Compliance with legal and contractual requirements	
A.18.1.1	Identification of applicable legislation and contractual requirements	Yes
A.18.1.2	Intellectual property rights	Yes
A.18.1.3	Protection of records	Yes
A.18.1.4	Privacy and protection of personally identifiable information	Yes
A.18.1.5	Regulation of cryptographic controls	Yes
A.18.2	Information security reviews	
A.18.2.1	Independent review of information security	Yes
A.18.2.2	Compliance with security policies and standards	Yes
A.18.2.3	Technical compliance review	Yes