Written Information Security Program (WISP)

The objectives of this comprehensive written information security program ("WISP") include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards Local Wërks ("LW') has selected to protect the personal and other sensitive information it collects, creates, uses, and maintains. LW does not physically collect or process personal information. No LW employees have access to personal information of customers.

1. Purpose. The purpose of this WISP is to:

(a) Ensure the security, confidentiality, integrity, and availability of personal and other sensitive information LW collects, creates, uses, and maintains;

(b) Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information;

(c) Protect against unauthorized access to or use of LW-maintained personal and other sensitive information that could result in substantial harm or inconvenience to any client or employee; and

(d) Define an information security program that is appropriate to LW size, scope, and business; its available resources; and the amount of personal and other sensitive information that LW owns or maintains on behalf of others, while recognizing the need to protect both client and employee information.

2. Scope. This WISP applies to all employees, contractors who are provided access to personal and sensitive information , officers, and directors of LW. It applies to any records that contain personal and other sensitive information in any format and on any media, whether in electronic or paper form.

(a) For purposes of this WISP, "personal information" means either a person's first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

(i) Social Security number;

(ii) Driver's license number, other government-issued identification number, including passport number, or tribal identification number;

(iii) Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account , and any personally identifiable financial information , description, or other grouping derived from personally identifiable financial information,

(iv) Biometric data collected from the individual and used to authenticate the individual during a transaction, such as an image of a fingerprint, retina, or iris; or

(v) Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

(b) Personal information does not include lawfully obtained information that is available to the public, including publicly available information from federal, state, or local government records.

(c) For purposes of this WISP, "sensitive information" means data that:

(i) LW considers to be highly confidential information; or

(ii) If accessed by or disclosed to unauthorized parties, could cause significant or material harm to LW, its clients, or its employees.

Sensitive information includes, but is not limited to, personal information.

Information Security Coordinator. LW has designated Rowdy Laughlin to implement, coordinate, and maintain this WISP (the "Information Security Coordinator"). The Information Security Coordinator shall be responsible for:

(d) Initial implementation of this WISP, including:

(i) Assessing internal and external risks to personal and other sensitive information and maintaining related documentation, including risk assessment reports and remediation plans ;

(ii) Coordinating the development, distribution, and maintenance of information security policies and procedures ;

(iii) Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal and other sensitive information ;

(iv) Ensuring that the safeguards are implemented and maintained to protect personal and other sensitive information throughout LW, where applicable ;

(v) Overseeing service providers that access or maintain personal and other sensitive information on behalf of LW ;

(vi) Monitoring and testing the information security program's implementation and effectiveness on an ongoing basis ;

(vii) Defining and managing incident response procedures ; and

(viii) Establishing and managing enforcement policies and procedures for this WISP, in collaboration with LW human resources and management.

(e) Employee training, including:

(i) Providing periodic training regarding this WISP, LW safeguards, and relevant information security policies and procedures for all employees who have or may have access to personal or other sensitive information;

(ii) Retaining records of training .

(f) Reviewing the WISP and the security measures defined herein at least annually, or whenever there is a material change in LW business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

(g) Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or LW information security policies and procedures.

(h) Periodically reporting to LW management regarding the status of the information security program and LW safeguards to protect personal and other sensitive information.

(i) Handling any customer complaints and compliance management

3. Risk Assessment. As a part of developing and implementing this WISP, LW will conduct a periodic, risk assessment, at least annually, or whenever there is a material change in LW business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

(a) The risk assessment shall:

(i) Identify reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of any electronic, paper, or other records containing personal or other sensitive information.

(ii) Assess the likelihood and potential damage that could result from such risks, taking into consideration the sensitivity of the personal and other sensitive information.

(iii) Evaluate the sufficiency of relevant policies, procedures, systems, and safeguards in place to control such risks, in areas that include, but may not be limited to:

(A) Employee training ;

(B) Employee compliance with this WISP and related policies and procedures;

(C) Information systems, including network, computer, and software acquisition, design, implementation, operations, and maintenance, as well as data processing, storage, transmission, retention, and disposal; and

(D) LW ability to prevent, detect, and respond to attacks, intrusions, and other security incidents or system failures.

(b) Following each risk assessment, LW will endeavor to :

(i) Design, implement, and maintain reasonable and appropriate safeguards to minimize identified risks.

(ii) Reasonably and appropriately address any identified gaps.

(iii) Regularly monitor the effectiveness of LW safeguards, as specified in this WISP.

4. Information Security Policies and Procedures. As part of this WISP, LW will develop, and maintain information security policies and procedures in accordance with applicable laws and standards and make them available to relevant employees, contractors, and others as necessary to:

(a) Establish policies regarding:

(i) Information classification;

(ii) Information handling practices for personal and other sensitive information, including the storage, access, disposal, and external transfer or transportation of personal and other sensitive information;

(iii) User access management, including identification and authentication (using 2-factor login procedures, passwords or other appropriate means);

(iv) End to End Encryption;

(v) Computer and network security;

(vi) Physical security;

(vii) Incident reporting and response;

(viii) Employee and contractor use of technology; and

(ix) Information systems acquisition, development, operations, and maintenance.

5. Safeguards. LW will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personal or other sensitive information that LW owns or maintains on behalf of others. Personal information of customers will be deleted no later than seven (7) days after submission.

(a) Safeguards shall be appropriate to LW size, scope, and business; its available resources; and the amount of personal and other sensitive information that LW owns or maintains on behalf of others, while recognizing the need to protect both client and employee information.

(b) LW administrative safeguards shall include, at a minimum:

(i) Designating one or more individuals to coordinate the information security program ;

(ii) Identifying reasonably foreseeable internal and external risks, and assessing whether existing safeguards adequately control the identified risks ;

(iii) Training employees in security program practices and procedures,

(iv) Selecting service providers that are capable of maintaining appropriate safeguards, and requiring service providers to maintain safeguards by contract ; and

(v) Adjusting the information security program in light of business changes or new circumstances ;

(c) LW technical safeguards shall include maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

(i) Secure user authentication protocols, including:

(A) Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords;

(B) Restricting access to active users and active user accounts only, including preventing terminated employees or contractors from accessing systems or records; and

(C) Blocking access to a particular user identifier after multiple unsuccessful attempts to gain access or placing limitations on access for the system.

(ii) Secure access control measures, including:

(A) Restricting access to records and files containing personal or other sensitive information to those with a need to know to perform their duties; and

(B) Assigning unique identifiers and passwords (or other authentication means) to everyone with computer or network access that are reasonably designed to maintain security.

(iii) Encryption of all personal or other sensitive information traveling wirelessly or across public networks as deemed reasonably necessary (with understanding that such protection may be waived upon the prior written approval and understanding of a specific client but only for that client's own personal and sensitive information).

(iv) Encryption of all personal or other sensitive information stored on laptops or other portable or mobile devices, and to the extent technically feasible, personal or other sensitive information stored on any other device or media (data-at-rest).

(v) Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to personal or other sensitive information or other attacks or system failures.

(vi) Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) personal or other sensitive information.

(vii) Reasonably current system security software (or a version that can still be supported with reasonably current patches and malware definitions) that (1) includes malicious software ("malware") protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

(d) LW physical safeguards shall, at a minimum, provide for:

(i) Defining and implementing reasonable physical security measures to protect areas where personal or other sensitive information may be accessed, including reasonably restricting physical access and storing records containing personal or other sensitive information in locked facilities, areas, or containers.

(ii) Preventing, detecting, and responding to intrusions or unauthorized access to personal or other sensitive information, including during or after data collection, transportation, or disposal.

(iii) Secure disposal or destruction of personal or other sensitive information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

6. Service Providers. LW will take reasonable steps to assure that service providers that may have access to or otherwise create, collect, use, or maintain personal or other sensitive information on its behalf follow reasonable information security measures consistent with this WISP and all applicable laws and LW obligations. LW uses Amazon Web Services (AWS).

7. Monitoring. LW will regularly test and monitor the implementation and effectiveness of its information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personal or other sensitive information. LW shall reasonably and appropriately address any identified gaps.

8. Access Management Policy for Payment Card Industry (PCI-DSS) LW will implement policies and procedures as reasonably necessary to comply with the Payment Card Industry (PCI-DSS) standards for collecting and using credit card holder data including an incident response plan in the event of a breach that could impact cardholder data.

9. Incident Response. LW will establish and maintain policies and procedures regarding information security incident response. Such procedures shall include:

(a) Documenting the response to any security incident or event that involves a breach of security;

(b) Performing a post-incident review of events and actions taken; and

(c) Reasonably and appropriately addressing any identified gaps.

10. Enforcement. Violations of this WISP may result in disciplinary action, in accordance with LW information security policies and procedures and human resources policies.

11. Program Review. LW will review this WISP and the security measures defined herein at least annually, or whenever there is a material change in LW business practices that may reasonably implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information.

12. Effective Date. This WISP is effective as of 01/01/2023.

(a) Revision History: [Original publication/[NOTE SUBSEQUENT REVISIONS]].