EXHIBIT F

INFORMATION TECHNOLOGY SECURITY

1. **Notification of Data Security Incident**

For purposes of this section, "Data Security Incident" is defined as unauthorized access to Peregrine's business and/or business systems by a third party, which access could potentially expose County data or systems to unauthorized access, disclosure, or misuse. In the event of a Data Security Incident, Peregrine must notify County **in writing as soon as possible and no later than 48 hours after Peregrine determines a Data Security Incident has occurred**. Notice should be made to all parties referenced in the "Notices" section of the Agreement. Notice must reference this contract number. Notice under this section must include the date of incident, Peregrine's systems and/or locations which were affected, and County services or data affected. The duty to notify under this section is broad, requiring disclosure whether any impact to County data is known at the time, to enable County to take immediate protective actions of its data and cloud environments.

Failure to notify under this section is a material breach, and County may immediately terminate the Agreement for failure to comply.

2. **Data Location**

2.1 Peregrine shall not store or transfer non-public County of Nevada data outside the United States. This prohibition includes backup data and Disaster Recovery locations. Peregrine will permit its personnel and contractors to access County of Nevada data remotely only as required to provide technical support. Remote access to data from outside the continental United States is prohibited unless expressly approved in advance and in writing by the County.

2.2 Peregrine must notify the County **in writing within 48 hours** of any location changes to Peregrine's data center(s) that will process or store County data. Notice should be made to all parties referenced in the "Notices" section of the Agreement.

3. **Data Encryption**

3.1 Peregrine shall encrypt all non-public County data in transit regardless of the transit mechanism.
3.2 Peregrine shall encrypt all non-public County data at rest.
3.3 Encryption algorithms shall be AES-128 or better.

4. **Cybersecurity Awareness and Training**

The County maintains a robust Cybersecurity Awareness and Training program intended to assist employees and contractors with maintaining current knowledge of changing cybersecurity threats and countermeasures. Any Peregrine employee or contractor that is assigned a County network account will be assigned User Awareness training and must complete it within the time period it is assigned. Training completion progress is monitored by sponsor departments and non-compliant users may have their account suspended or restricted.

The County conducts email Phish testing on a regular basis to expose account holders to the types of potential threats.

Peregrine will maintain a Cybersecurity Awareness and Training program for training staff at a minimum of once a year. Peregrine will maintain records of the program for review by the County when requested.

5. **Artificial Intelligence use**

5.1 Definitions:

Artificial Intelligence Technology (AI Technology): includes any machine learning, deep learning, or artificial intelligence ("AI") technologies, such as statistical learning algorithms, models (including large

language models), neural networks, and other AI tools or methodologies, as well as all software implementations and related hardware or equipment capable of generating content (e.g., text, images, video, audio, or computer code) based on user-supplied prompts.

County Data: includes all information, data, materials, text, prompts, images, or other content provided to Peregrine under this Agreement or any other agreements between Peregrine and the County.

5.2 Responsibilities and Training:

Peregrine is responsible for all information in the machine learning model, intellectual property rights associated with the information, and software and coded instructions used to generate AI content, to the extent those machine learning models are under Peregrine's sole use and control. County is responsible for the accuracy, utility and formulation of prompts and other inputs used to access the AI services and for decisions made, advice given, actions taken, and failures to take action based on AI content generated from AI services, except for AI content that is generated from erroneous or non-existing information in Peregrine's machine learning models or from malfunctioning AI service software.

The County acknowledges that Peregrine only uses commercially available machine learning models in its deployment of the Service and exercises no authority or control over the training, development, or tuning of those machine learning models. With regard to any machine learning models under Peregrine's sole use and control, Peregrine shall not use, or permit any third party to use, County Data to train, validate, update, improve, or modify any AI Technology, whether for Peregrine's benefit, without the County's prior written authorization, which the County may grant or withhold at its sole discretion.

EXHIBIT F(a)

LIST OF APPROVED INDIVIDUALS WORKING OUTSIDE THE CONTINENTAL UNITED STATES

Pursuant to § 2.1 of Exhibit F, Information Technology Security, the following individuals located outside the continental United States are approved to access County of Nevada data remotely, as required to provide technical support:

- Javier Wilson, Cloud Infrastructure Engineering Team Manager – Ottawa, Ontario, Canada