PRIVACY POLICY

iPledgeNow, Inc. (the "**company**", "**we**" or "**us**") is committed to protecting the confidentiality of data in its possession. This policy sets forth the expectations of the company related to the receipt, handling, storage, use, transmission and destruction of confidential or protected data. This policy applies to the company; its employees, agents and representatives; and vendors and others that receive, use, store or transmit information on the company's behalf.

We are and may in the future be subject to various data protection laws, both foreign and domestic. Such laws have certain common principles and elements, which we respect and will uphold, including (1) transparency, (2) limiting the collection of data, (3) allowing data subjects to have a say in how their personal data is stored and used, (4) implementation reasonable physical, technical and administrative safeguards to prevent unauthorized access or use of protected data, (5) ongoing risk assessment, and (6) vigilance in preventing and responding to data breaches.

This policy describes our current privacy policy, which are subject to periodic change. Questions regarding this policy should be addressed to the **Data Protection Officer** identified in this policy.

DEFINITIONS

"Personal Information" means information that relates to an identifiable natural person or that can be used, by itself or combined with other data, to identify that person, regardless of whether the information is confidential or publicly available. This includes both business and personal information. Examples of Personal Information include name, address, telephone number, email address, business contact information, business affiliation, title, etc. Personal Information also includes all Sensitive Personal Information (as defined below). Personal Information does not include information about an individual that cannot be used to identify that individual, including in combination with other data, such as aggregated and deidentified data.

"Confidential Information" means confidential, proprietary or trade secret information of or about us or our products; confidential, proprietary and trade secret information of third parties entrusted to us; and information that a reasonable person would believe should be treated as confidential. Questions regarding whether specific data or information is confidential should be directed to the Data Privacy Officer.

"Data Protection Officer" means the individual authorized and obligated to enforce and interpret this policy and for the overall protection and management of our data. The Data Privacy Officer is Bob Dankert.

"Protected Information" means all Personal Information, Confidential Information, Sensitive Personal Information, and all other information that the Data Privacy Officer designates as subject to this policy.

"Sensitive Personal Information" means Personal Information that is especially sensitive and that should be treated with additional respect and protection, often because its improper use or transmission can lead to identity theft or other significant losses. Examples of Sensitive Personal Information include Social Security Number (SSN); National Insurance Number (NI); credit card number; bank account number(s); username(s) and/or password(s); health information, genetic and biometric information; Personal Information of children; and criminal history, as well as information regarded as highly private or sensitive

under various laws, such as information regarding race, ethnicity, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientation. Questions regarding whether specific data or information constitutes Sensitive Personal Information should be directed to the Data Privacy Officer.

"Breach" means an unauthorized use or disclosure of Protected Information, including without limitation unauthorized access. While an unprotected transmission of Protected Information may result in a Breach, it is not, by itself, a Breach.

"Data Subject" means an individual to whom Personal Information or Sensitive Personal Information pertains.

PERSONAL INFORMATION

DATA PROTECTION PRINCIPLES

The following principles govern our collection, use, retention, transfer, disclosure and destruction of Personal Information:

1. Lawfulness, Fairness and Transparency: Personal Information will be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means we will inform Data Subjects how we obtain and use their data (primarily through our Privacy Policy on our website), the use must match the descriptions given to the Data Subject, and it must be for a purpose allowed by applicable law.

2. Purpose Limitation: Personal Information will be collected specific and legitimate purposes and not further used in a manner that is incompatible with those purposes. This means we will know why we are obtaining Personal Information when we obtain it and we will not use it for other purposes without consent or other lawful basis to do so.

3. Minimum Necessary: We do not collect Personal Information we do not need and we will only retain it as long as we have a legitimate need for it. We only collect, maintain, use and transmit the minimum amount of Protected Information necessary to accomplish a given task, and we only allow the least amount of people the lowest amount of access necessary to accomplish a specific purpose.

   We collect primarily the information you supply us with as well as your IP address and the number of times you take the Pledge.

4. Accuracy: Personal Information should be accurate and kept up to date. We will have in place a process to correct and update information and to receive and act upon requests from Data Subjects to correct their information.

5. Access Limitation: Personal Information will only be accessible to those with a legitimate need for the information to accomplish a permissible purpose. This includes both protection from external access and internal limitations on who within the company can access Personal Information.

6. Integrity & Confidentiality: Personal Information will be received, maintained, used and/or transmitted in a matter that ensures appropriate security, including protection from unauthorized

or unlawful access, as well as accidental loss, destruction or damage. Data Subjects will be afforded their rights as recognized under applicable laws (including GDPR and CCAP where applicable).

DATA COLLECTION

We will not obtain the Personal Information of any individual unless you supply it to us or otherwise take the Pledge, and then only an IP address.

Most Personal Information we receive is provided directly by the Data Subject, and in most cases the providing of such information is specifically so that we may use the information to further its relationship with the individual. Where it is clear that is the intent, no further permission is required. In some cases, it may be necessary to obtain an individual's affirmative consent before collecting or using their Personal Information further, such as the requirement that users of our website affirmatively agree to our use of "cookies" or where we are entrusted with Sensitive Personal Information for limited purposes, such as processing investments or providing tax information. If there is reason to doubt whether the Data Subject consents to use of their personal information to contact them, ask.

RIGHTS OF DATA SUBJECTS

We respect the rights of individuals to control their Personal Information under various laws, and we will allow them to exercise those rights. Subject to applicable laws (including employment laws and record retention requirements) all Data Subjects have the right to:

1. access information about them that we have.
2. correct any Personal Information about them that we have.
3. request that we delete their personal information.
4. request that we limit the way we use or share their Personal Information.
5. object to use of their Personal Information for direct marketing.

All requests from a Data Subject related to these rights should be forwarded to the Data Protection Officer, who will respond accordingly. The Data Protection Officer will undertake reasonable efforts to authenticate the identity of the requesting individual before providing further information or undertaking further action to allow the individual to exercise one or more of the above rights. There may be situations where someone other than the Data Subject requests Personal Information of another, such as requests by police or court order. All such requests should be forwarded to the Data Protection Officer, who will respond accordingly.

DATA SECURITY

No information, especially electronically stored or transmitted information, is absolutely safe. However, we take the protection of Personal Information, Confidential Information and all other Protected Information seriously. We will continue to actively assess risks and look for ways to better safeguard Protected Information.

We protect Protected Information through physical, technical and administrative safeguards, taking into account factors such as legal requirements; the sensitivity of the information; the need for and uses pertaining to it; practical factors related to access, use and cost; foreseeable risks, their likelihood and the potential harm were breach of the information to occur.

WHO TO CONTACT

Questions and concerns regarding this policy, its application or interpretation, security and accessibility of our data and other related matters should be directed to the Data Protection Officer:

Bob Dankert
Director of Software Engineering
608-824-2076
bob.dankert@envisionitllc.com