UFP Technologies, Inc

Information Security

RESPONSIBILITIES:

The Board of Directors of UFP Technologies has delegated responsibility of discussing and evaluating the Corporation's policies with respect to risk assessment and risk management as well as the Corporation's significant areas of financial risk exposure and steps management takes to monitor and control such exposures to the Audit Committee of the Board of Directors.

Information Security risks are included in the Information Technology risk assessment subsection of the Company's Risk Assessment. The Corporation's executive team works with the Vice President of Information Technology who has primary responsibility to design and administer the policies and practices in place to protect the information, applications and hardware utilized by the Corporation to process transactions and accumulate and store data. The VP of IT attends Audit Committee meetings annually and as needed to brief the Committee on Information Security matters including any cyber breaches and the impact of such. The VP of IT presents the latest safeguards in place to prevent cyber breaches and the preparedness of the department and steps designed to be followed in the event of a breach. The VP of IT is brought into additional Audit Committee meetings to discuss other pertinent cyber security topics as they may arise. The VP of IT also meets with external IT auditors a couple of times per year to support the audit efforts of that team which include documenting controls related to Cyber Security. Internal Audit of the Corporation tests the Information Technology General Controls and Policies as part of the annual Audit Plan.

INSURANCE:

The Corporation has a cyber security insurance policy. The SVP of Finance & CFO and the Corporate Controller review all insurance policies and coverages and review with the Audit Committee annually and as needed.

POLICY:

The Corporation has a Cyber Security Policy in place that is updated by the IT Department annually and reviewed and approved by the SVP of Finance and CFO of the Corporation. The Cyber Security Policy describes the policies and procedures in place designed to protect the critical information and technology resources of the Corporation and includes descriptions of the threats to those IT assets. The Policy also includes a Cyber Incident Response plan component.

TRAINING:

All employees review and sign acknowledgement of the Corporation's "IT Acceptable Use Policy" and attend formal training for GDPR, Controlled Unclassified Information handling, and Insider Threat/ Incident Reporting related to the Corporations security practices. Updated training is provided.

RECENT BREACHES:

2020 – The Corporation experienced no significant cyber breaches

2019 – The Corporation experienced no significant cyber breaches

2018 – The Corporation experienced no significant cyber breaches

The Corporation has incurred $0 net expenses related to information security breach penalties and settlements.