**Information Security:**

As a trusted member of our organization, your understanding of our Information Security Policy is vital to ensuring the safety and integrity of our shared digital resources. Guided by the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, we have implemented an Information Security Management System (ISMS) that lays the groundwork for our digital protection efforts.

Outlined below are the core elements of our ISMS:

* **Identify:** Our first step in maintaining security involves recognizing all the digital assets that need protection. This means knowing our hardware, software, and data inside and out—what they do, who uses them, and how they might be vulnerable to threats. We encourage everyone to be mindful of the digital resources they use and understand their value.
* **Protect:** Once we've identified what needs protection, we set up safeguards. This includes everything from limiting data access to those who need it, using strong passwords, and keeping our systems updated and patched. We ask that you follow all protection protocols in place and report any potential weaknesses you may notice.
* **Detect:** Quick detection of threats is crucial. We use monitoring and detection systems to identify any unusual activity, and we count on you to report anything suspicious.
* **Respond:** If a security incident does occur, we have a response plan in place. This includes specific procedures to mitigate the incident, ensure effective communication, and get systems back up and running. In such events, it's crucial to follow the instructions of our IT team promptly.
* **Recover:** In the wake of any incident, our aim is to recover and restore any affected systems or services. We learn from these events to prevent future occurrences.

Additionally, we are committed to the Service Organization Control (SOC) reporting standards. This ensures we maintain transparency about our security efforts and keep our security controls up-to-date.