This Cybersecurity Policy provides information regarding our cybersecurity risk management, strategy, and governance, along with a related description of our information security and data privacy practices. Securing company systems, business information, and personal information of our guests, team members, vendors, and other third parties is important to us.

We have systems in place to:

- safely receive, protect, and store information;
- collect, use, and share that information appropriately; and
- detect, contain, and respond to information security, cybersecurity, and data privacy incidents.

While everyone at Once Upon a Farm, PBC plays a part in information security, cybersecurity, and data privacy, oversight responsibility is shared by our Board of Directors, its Audit Committee and Management.

Governance and Responsibility

To inform and educate the Board of Directors in its primary oversight responsibility for information security, cybersecurity, and data privacy, Management provides updates on these topics. For example, the VP of IT and Systems addresses information security risks and controls, cyber threats, and other program updates, and senior members of the risk team provide enterprise risk management program updates. In addition, the Board of Directors receives updates from Management regarding Once Upon a Farm's overall risks, which include risks related to these topics.

Roles and responsibilities

Responsible party	Oversight of information security, cybersecurity, and data privacy
Board of Directors	Oversight of these topics within Once Upon a Farm's overall risks.
Management	Our technology leadership provides regular updates on cybersecurity and data privacy to our Board's Audit Committee.
Third-Party Vendors	Advisory services, threat intelligence, 24/7 monitoring, vulnerability scanning, security and penetration testing, control audits.

Integration into Enterprise Risk Management Program

By aligning the identification, assessment, and management of risks related to information security, cybersecurity, and data privacy with our overall approach to risk oversight by the Board of Directors, its committees, and Management, we have integrated these practices into our enterprise risk management program.

Management Expertise

Our VP of IT and Systems leads the strategic direction and management of Once Upon a Farm's enterprise technology systems, is responsible for Once Upon a Farm's technology roadmap and oversees the infrastructure, cybersecurity, data sciences, and architecture teams. He has held a variety of technology leadership roles and has developed significant knowledge and skills regarding enterprise technology systems, including cybersecurity. Our Director of IT has a strong background in technology, information security, cybersecurity, risk management, audit, and compliance.

Systems and Processes

We use a combination of industry-leading tools to protect Once Upon a Farm and our guests, operate a proactive threat intelligence program to identify and assess risks, including threats associated with our use of third-party service providers.

Our program is based on recognized industry security standards and control frameworks, which we seek to validate through internal and independent assessments. Our cybersecurity team regularly tests our controls through penetration testing, vulnerability scanning, and attack simulation. In addition, we have an incident response program to address potential security and privacy incidents. As part of this incident response program, members of Management are informed about and monitor the prevention, detection, mitigation, and remediation of potential security and privacy incidents. The program uses a coordinated escalation model to provide information to, and engage with, relevant members of Management and the Board of Directors, as needed, throughout the incident response process.

Regular Training and Compliance

We believe that security is every employee's responsibility. Our team members receive regular, role-specific training to help them recognize and respond to threats.

Use of Third Parties

Beyond our in-house capabilities we engage with leading security and technology vendors to assess our information security and cybersecurity program; provide threat intelligence; staff our Security Operations Center; and test our technical capabilities.

Vendor Risk Management

We evaluate the security practices of our third-party vendors as part of our onboarding and an ongoing vendor management process.

Insurance Coverage

We maintain insurance coverage intended to limit our exposure to certain network security and privacy matters.

Disclaimer

While we maintain robust cybersecurity programs and controls, no system can be completely secure. We continually assess and adapt our approach to mitigate evolving threats.