INFORMATION TECHNOLOGY AND CYBER SECURITY POLICY

TEXAS PACIFIC LAND CORPORATION

Texas Pacific Land Corporation (together with its subsidiaries, the "Company") is committed to ensuring cyber and the integrity of its information technology systems and data. This Information Technology and Cyber Security Policy (this "Policy") is designed as a formal set of guidelines for accessing the Company's technology and information ("IT") systems and to protect and identify threats to IT and cyber security. This Policy does not reflect all cyber security and IT policies and procedures of the Company, certain of which are set forth in other policies that are available either in the Code of Business Conduct and Ethics, Employee Handbook or upon request directed to the Company's General Counsel or Human Resources.

Governance of IT & Cybersecurity

TPL is committed to the continuous, proactive management of our IT and cybersecurity policies and processes. While cyber threats continue to evolve, the Company remains steadfast in our oversight and management of these issues. Adhering to holistic and stringent cybersecurity practices is a commitment that all TPL employees support in their day-to-day responsibilities. Our governance starts at the top of the organization. IT and Cybersecurity governance is ultimately overseen by the Audit Committee of the Board of Directors and implemented and maintained by Executive Leadership, including the Chief Executive Officer ("CEO"), Chief Financial Officer, Chief Accounting Officer and General Counsel. Throughout the year, the Audit Committee receives periodic IT and cybersecurity updates unless there is a notable event that requires immediate communication.

TPL Executive Leadership has existing policies/procedures in place that are updated and reviewed regularly to respond to security threats or breaches. Our policies and procedures outline our preventative programs and practices, including:

- Security incident response plan
- Configuration standards
- Change control process
- GAIT for Business and IT risk plan
- Disaster recovery plan
- IT acceptable use policies and procedures
- Patching policy

Equally as critical is our Executive Leadership. On a regular basis, Executive Leadership meets with the Director of IT to discuss a range of critical business updates, reporting, and disclosures, including cybersecurity considerations, ensuring the proper alignment with business risks and opportunities for innovation is in balance.

Executive Leadership has also created a formal governing committee to make critical IT strategic decisions and provide leadership direction. The Company has an IT Committee that meets quarterly and actively manages the oversight and decision making around the company's security strategy. This committee is comprised of the CFO, CAO, the Director of IT, the Director of Internal Audit, the Director of HR, and an outsourced Security Administration Lead. This team reviews issues, observations, trends, and the results presented by multiple monitoring reports.

TPL engages a third-party company to act as an outsourced functional IT service provider. Their services range from internal issue resolution, security consultation, cybersecurity due diligence protocols, business

continuity, and standards recommendation. The third-party security administration lead participates in the Company's IT Committee meetings to provide insight and awareness into reports, current threats, and the Company's efforts to mitigate risks related to those threats. They are also in constant communication with the Company's Executive Leadership —this direct line of contact with the Company's leadership ensures that immediate action can be taken, including the allocation of capital to new infrastructure or software, to continue protecting the integrity of our data, technology and related infrastructure. The Director of IT partners with the outsourced IT service provider to evaluate and escalate issues through the IT Committee as they occur following the security incident response plan and protocols.

The Director of IT oversees and manages the relationship with the IT service provider and is the point of contact for engagement. The IT service provider ensures the integrity and security of our IT systems. They obtain, assess, and submit SOC2 reports for relevant IT applications to the Director of IT as they are available. As additional applications are procured, Executive Leadership assesses the business criticality of each and the appropriate risk response. Additionally, the IT Committee monitors performance of the IT service provider monthly. These reviews allow management to assess the IT service provider's performance as it pertains to timeliness of ticketing responses, threat activity responses, security access, and change control.

TPL Information Security Management System

TPL has a series of safeguards in place to monitor new and evolving cybersecurity threats. In addition to vulnerability and penetration testing, management reviews Cybersecurity and Infrastructure Security Agency (CISA) monitoring and threat reports, to assist in identifying any new risks and threats that could impact the company. Other critical prevention measures include:

- Endpoint detection and response
- Antivirus software
- Firewalls and web proxies
- Two-factor authentication
- Daily and real-time Server backups and DR plan to meet RPO/RTO
- Annual external and internal penetration testing
- Managed patching policies
- Change management policies

TPL IT Environment Evaluation Program

As stated above, TPL partners with an external IT firm to conduct an annual evaluation of our IT environment. This independent, third-party evaluation of our existing IT environment is functioning to our high-security standards.

The Company performs regular due diligence across our applications, databases, servers, and infrastructure. Our IT Risk Assessment considers all of these and evaluates each one, individually. Each item assessed is given a business criticality ranking and consideration is given to how each would be affected, considering the likelihood and impact, from change management, operating failure, and security failure perspectives. Risk responses are determined from these factors.

TPL Formal IT Training Programs (required of all TPL employees)

TPL employees are required to complete annual information security training, in addition to other training requirements. The result is an educated, informed, and prepared workforce, with an awareness of potential cybersecurity threats, how they may occur, identification of various situations, and how to report

and escalate. These training efforts are supplemented with regular corporate-led communications and outreach initiatives to continue to facilitate cybersecurity awareness and ensure the TPL team remains vigilant and informed about cybersecurity threats and trends. Constant awareness campaigns and annual training expectations equip our workforce with the tools to respond quickly and appropriately to threats, facilitate continued security awareness and protection. The Company has a series of IT and Cybersecurity policies and procedures that are reviewed at least annually to verify accuracy and compliance, including a robust Security and Incident Response Plan. Our training and programs include:

- Annual, mandatory recertification of IT acceptable use policies and procedures for all employees and contractors.
- Annual mandatory IT security training for all employees, including the following topics:
    - □ IOT/Connected devices/mobile devices expectations and training
    - □ Phishing
    - □ Passwords/MFA
    - □ External devices/physical access
    - □ Insider threats
    - □ Social engineering
    - □ 3rd party applications
    - □ Active SPAM system