LINEAGE
CELL THERAPEUTICS

INFORMATION SECURITY STATEMENT

Information is a critical asset to our business. With much of our information stored electronically, this asset is vulnerable to cyberattacks that could disrupt our operations and compromise the security of business and personal information that the Company is bound to protect. Attacks of this nature are being conducted by sophisticated and organized actors, and are occurring with greater frequency, persistence, complexity and intensity.

Lineage is committed to information security, including cybersecurity, and the protection against malicious breaches that could adversely affect our business, employees, investors, and other stakeholders. Our cybersecurity strategy prioritizes both detection and response to cyber threats, as well as resilience against such incidents. We maintain a formal cybersecurity program for our U.S. operations, and we intend to adopt similar measures globally in the future. Our program includes the following practices, among others:

- Prioritizing vigilance in the identification and monitoring of current risks related to information security and taking the necessary steps to minimize these risks.
- Continuously evaluating and making prudent investments in our information security detection and response capabilities.
- Retention of an industry leading consulting firm to conduct an independent assessment of our information security policies, systems, and controls to evaluate our cybersecurity readiness against NIST standards.
- Reviewing our information security (including cybersecurity) policies, systems, and controls with the Audit Committee of the Board of Directors on a quarterly basis, and with our entire Board periodically. Each of the directors serving on the Audit Committee possesses relevant experience in information systems and security.
- Maintaining a robust, mandatory training program for employees that includes ongoing security awareness training and testing.
- Defining appropriate use of electronic communications and providing clear guidance for employees on the use of email, internet and social media sites to ensure that sensitive information is appropriately handled and protected.
- Conducting ongoing simulated penetration tests and mock phishing attacks to assess the effectiveness of our controls and the alertness of our employees.
- Utilizing role-based access controls (RBAC), which restrict network access to only what is required for the individual’s role within the organization.
- Maintaining robust security systems for use and processing of personal information to ensure this information is secured against unauthorized access and disclosure. See our Privacy Policy (link to our privacy policy on the website) for additional information regarding how we handle personal information.
- Maintaining a dedicated information security risk insurance policy, with ransomware coverage and breach response services.
- Continuously evaluating the requirements of Sarbanes Oxley related to our IT environment and general IT controls surrounding the Company’s financial reporting.