Cybersecurity Policy

1. Purpose

The purpose of this Cybersecurity Policy is to protect the company's information systems, business data, customer information, and any Federal Contract Information (FCI) from unauthorized access, disclosure, alteration, or destruction. This policy, which is supplemental to the "Oak Therapeutics IT and Information Safeguarding Policy", establishes minimum cybersecurity requirements for all employees, contractors, consultants, temporary workers, and third parties who access company systems or data. This policy is aligned with the safeguarding principles outlined in FAR 52.204-21, including access control, malware protection, physical security, system monitoring, authentication, and secure handling of information.

2. Scope

This policy applies to:

- All company-owned devices, systems, networks, and cloud services
- All employees and contractors
- All information created, processed, stored, or transmitted by the company
- Remote work environments and mobile devices used for company business

3. Roles and Responsibilities

3.1 Management. Management is responsible for:

- Supporting cybersecurity efforts
- Providing appropriate resources
- Enforcing compliance with this policy

3.2 Employees and Users. Users are responsible for:

- Following this policy
- Protecting passwords and devices
- Reporting suspicious activity immediately
- Completing required cybersecurity awareness training

3.3 IT or Managed Service Providers (MSPs). IT personnel or service providers are responsible for:

- Maintaining security systems
- Applying software updates and patches
- Monitoring systems for threats
- Responding to cybersecurity incidents

4. Access Control

- Access to systems and data shall be limited to authorized users only.
- Users shall only receive access necessary for their job responsibilities ("least privilege").
- Shared accounts are prohibited unless specifically approved.
- User accounts shall be disabled promptly upon employee termination or role change.
- Multi-factor authentication (MFA) shall be enabled wherever feasible, especially for:
    - Email systems
    - Remote access
    - Administrative accounts
    - Cloud services

5. Password Requirements

- Passwords must be unique and difficult to guess.
- Minimum password length shall be 12 characters where supported.
- Password sharing is prohibited.
- Default passwords on systems and devices must be changed immediately.
- Password managers are strongly encouraged.

6. Device and System Security

- Company devices must use up-to-date antivirus or endpoint protection software.
- Operating systems and applications must be updated regularly.
- Unsupported or end-of-life software may not be used unless approved by management.
- Screen locks must activate automatically after periods of inactivity.
- Company data should not be stored on personal devices unless authorized.

7. Network Security

- Firewalls shall be used to protect company networks.

- Wireless networks must use encryption and strong passwords.
- Public-facing systems should be separated from internal company systems whenever feasible.
- Remote access must occur through secure methods such as VPNs or approved cloud security solutions.

8. Protection Against Malware

- Antivirus and anti-malware protections must remain enabled at all times.
- Email attachments and downloads from unknown sources should not be opened.
- Systems shall be scanned regularly for malicious software.
- Security tools shall be updated when new releases become available.

9. Data Protection and Disposal

- Sensitive business and customer information shall be stored securely.
- Data should be backed up regularly.
- Portable media containing sensitive information must be encrypted where possible.
- Electronic media must be securely erased or destroyed before disposal or reuse.

10. Physical Security

- Physical access to systems, servers, and networking equipment shall be restricted to authorized personnel.
- Visitors must be escorted in restricted areas.
- Employees are responsible for securing laptops and mobile devices when traveling or working remotely.

11. Incident Reporting and Response

Employees must immediately report:

- Suspected phishing emails
- Malware infections
- Lost or stolen devices
- Unauthorized access attempts
- Data breaches or suspicious system activity

Management or IT personnel shall:

- Investigate incidents promptly
- Contain and remediate threats
- Document significant incidents
- Notify affected parties when required by law or contract

12. Security Awareness Training

All employees shall receive periodic cybersecurity awareness training covering topics such as (but not limited to):

- Password security
- Phishing and social engineering
- Safe internet and email use
- Data handling procedures
- Incident reporting requirements

All users are required to take, at the minimum, one of the following trainings annually and / or review the following resources:

- U.S. Cybersecurity and Infrastructure Agency: https://learning.cisa.gov/login/index.php (choose "Cyber Essentials")
- National Cybersecurity Alliance: https://www.staysafeonline.org (choose "Managing Cyber Risk at Your Small Business")
- Federal Trade Commission Cybersecurity for Small Business: https://www.ftc.gov/business-guidance/small-businesses/cybersecurity (choose "Cybersecurity Basics")
- Microsoft Cybersecurity 101: https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity (choose Cybersecurity 101).

13. Third-Party Service Providers

Third-party vendors or contractors with access to company systems or sensitive information must:

- Follow appropriate cybersecurity practices
- Maintain reasonable security controls
- Report security incidents affecting company information promptly

14. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

15. Policy Review

This policy shall be reviewed at least annually and updated as needed to address evolving cybersecurity risks, legal requirements, and business operations.

Policy Signed and Adopted:	6/1/2026
By:	Gerhard Apfelthaler, Chief Business Officer
Next Policy Review Due on:	5/31/2027