ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in:

(1) Substantial harm to the adviser, or

(2) Substantial harm to a client, or an investor in a private fund, whose information was accessed.

Significant fund cybersecurity incident has the same meaning as in § 270.38a-2 of this chapter (rule 38a-2 under the Investment Company Act of 1940).

22. Section 275.206(4)-9 is added to read as follows:

§ 275.206(4)-9 Cybersecurity policies and procedures of investment advisers.

(a) *Cybersecurity policies and procedures*. As a means reasonably designed to prevent fraudulent, deceptive, or manipulative acts, practices, or courses of business within the meaning of section 206(4) of the Act (15 U.S.C. 80b6(4)), it is unlawful for any investment adviser registered or required to be registered under section 203 of the Investment Advisers Act of 1940 (15 U.S.C. 80b-3) to provide investment advice to clients unless the adviser adopts and implements written policies and procedures that are reasonably designed to address the adviser's cybersecurity risks, including policies and procedures that:

(1) *Risk assessment*.

(i) Require periodic assessments of cybersecurity risks associated with adviser information systems and adviser information residing therein, including requiring the adviser to:

(A) Categorize and prioritize cybersecurity risks based on an inventory of the components of the adviser information systems and adviser information residing therein and the potential effect of a cybersecurity incident on the adviser; and

(B) Identify the adviser's service providers that receive, maintain, or process adviser information, or are otherwise permitted to access adviser information systems and any adviser information residing therein, and assess the cybersecurity risks associated with the adviser's use of these service providers.

(ii) Require written documentation of any risk assessments.

(2) *User security and access*. Require controls designed to minimize user-related risks and prevent unauthorized access to adviser information systems and adviser information residing therein, including:

(i) Requiring standards of behavior for individuals authorized to access adviser information systems and any adviser information residing therein, such as an acceptable use policy;

(ii) Identifying and authenticating individual users, including implementing authentication measures that require users to present a combination of two or more credentials for access verification;

(iii) Establishing procedures for the timely distribution, replacement, and revocation of passwords or methods of authentication;

(iv) Restricting access to specific adviser information systems or components thereof and adviser information residing therein solely to individuals requiring access to such systems and information as is necessary for them to perform their responsibilities and functions on behalf of the adviser; and

(v) Securing remote access technologies.

(3) *Information protection*.

(i) Require measures designed to monitor adviser information systems and protect adviser information from unauthorized access or use, based on a periodic assessment of the adviser information systems and adviser information that resides on the systems that takes into account:

(A) The sensitivity level and importance of adviser information to its business operations;

(B) Whether any adviser information is personal information;

(C) Where and how adviser information is accessed, stored and transmitted, including the monitoring of adviser information in transmission;

(D) Adviser information systems access controls and malware protection; and

(E) The potential effect a cybersecurity incident involving adviser information could have on the adviser and its clients, including the ability for the adviser to continue to provide investment advice.

(ii) Require oversight of service providers that receive, maintain, or process adviser information, or are otherwise permitted to access adviser information systems and any adviser information residing therein and through that oversight document that such service providers, pursuant to a written contract between the adviser and any such service provider, are required to implement and maintain appropriate measures, including the practices described in paragraphs (a)(1), (a)(2), (a)(3)(i), (a)(4), and (a)(5) of this section, that are designed to protect adviser information and adviser information systems.

(4) *Cybersecurity threat and vulnerability management*. Require measures to detect, mitigate, and remediate any cybersecurity threats and vulnerabilities with respect to adviser information systems and the adviser information residing therein;

(5) *Cybersecurity incident response and recovery*.

(i) Require measures to detect, respond to, and recover from a cybersecurity incident, including policies and procedures that are reasonably designed to ensure:

(A) Continued operations of the adviser;

(B) The protection of adviser information systems and the adviser information residing therein;

(C) External and internal cybersecurity incident information sharing and communications; and

(D) Reporting of significant cybersecurity incidents under Rule 204-6 (17 CFR 275.204-6).

(ii) Require written documentation of any cybersecurity incident, including the adviser's response to and recovery from such an incident.

(a) *Annual Review*. An adviser must, at least annually:

(1) Review and assess the design and effectiveness of the cybersecurity policies and procedures required by paragraph (a) of this section, including whether they reflect changes in cybersecurity risk over the time period covered by the review; and

(2) Prepare a written report that, at a minimum, describes the review, the assessment, and any control tests performed, explains their results, documents any cybersecurity incident that occurred since the date of the last report, and discusses any material changes to the policies and procedures since the date of the last report.

(b) *Definitions*: For purposes of this section:

Adviser information means any electronic information related to the adviser's business, including personal information, received, maintained, created, or processed by the adviser.

Adviser information systems means the information resources owned or used by the

adviser, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of adviser information to maintain or support the adviser's operations.

Cybersecurity incident means an unauthorized occurrence on or conducted through an adviser's information systems that jeopardizes the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

Cybersecurity risk means financial, operational, legal, reputational, and other consequences that could result from cybersecurity incidents, threats, and vulnerabilities.

Cybersecurity threat means any potential occurrence that may result in an unauthorized effort to adversely affect the confidentiality, integrity, or availability of an adviser's information systems or any adviser information residing therein.

Cybersecurity vulnerability means a vulnerability in an adviser's information systems, information system security procedures, or internal controls, including vulnerabilities in their design, configuration, maintenance, or implementation that, if exploited, could result in a cybersecurity incident.

Personal information means:

(1) Any information that can be used, alone or in conjunction with any other information, to identify an individual, such as name, date of birth, place of birth, telephone number, street address, mother's maiden name, Social Security number, driver's license number, electronic mail address, account number, account password, biometric records or other nonpublic authentication information; or

(2) Any other non-public information regarding a client's account.