2876.3055 PROTECTION OF PURCHASER INFORMATION.

Subpart 1. **Cybersecurity policy.**

A. Portal operators and MNvest issuers must take reasonable steps to ensure that purchasers' financial and personal information is properly secured. Reasonable steps include, at a minimum, a written cybersecurity policy that outlines the MNvest issuer's or portal operator's policies and procedures for:

(1) preventing cybersecurity attacks that result in the disclosure, or potential disclosure, of purchasers' confidential or personally identifiable information;

(2) preventing data breaches that result in the disclosure, or potential disclosure, of purchasers' confidential or personally identifiable information;

(3) responding to a cybersecurity attack or data breach that occurs; and

(4) demonstrating the issuer's implementation of the written cybersecurity policy.

B. The cybersecurity policy required in item A must specifically include the MNvest issuer's or portal operator's procedures to establish compliance with Minnesota Statutes, section 325E.61.

C. MNvest issuers and portal operators must publish the cybersecurity policy required by this subpart on the portal operator's or MNvest issuer's website, with a prominent link to the cybersecurity policy on the website's homepage.

Subp. 2. **Reporting of a cybersecurity attack or data breach.** MNvest issuers and portal operators must report to the administrator any action taken by the MNvest issuer or portal operator to meet the reporting requirements of Minnesota Statutes, section 325E.61.

A. The report sent to the administrator must not include any confidential or personally identifiable information of those individuals whose data were improperly accessed or acquired, unless the information is requested by the administrator. The report must include:

(1) a general description of the type of data that were accessed or acquired;

(2) the number of individuals whose data were improperly accessed or acquired; and

(3) a description of the steps taken by the MNvest issuer or portal operator to notify the individuals whose data were improperly accessed or acquired.

B. The report must be mailed or sent electronically to the administrator within 60 days of the MNvest issuer's or portal operator's discovery of the cybersecurity attack or data breach.

Statutory Authority: *MS s 45.023; 80A.82*

History: *40 SR 1617*

Published Electronically: *September 6, 2018*