Domain #7

Risk Management

Community Care Durham
SUPPORTING PEOPLE, STRENGTHENING COMMUNITY

Pursuing Excellence,
Stepping into the future with pride!

7.1

A risk assess mentor risk management report is developed, is reviewed at regular intervals to minimize the organization's exposure to risk or liability, and includes:

- a. the identification of key and emerging risks
- b. an analysis of the likelihood of risk and/or the level of risk
- c. the identification of preventive controls and/or detection controls
- d. the ongoing implementation, monitoring, and evaluation of action plan(s)to mitigate risks
- e. the allocation of resources to mitigate risk

7.2

A business continuity plan is developed based on the organization's mission and strategic directions/goals, and outlines:

- a. potential threats facing the organization that are critical to operations and/or service delivery
- b. emergency preparedness and responses to various threats that affect operations and/or service delivery
- c. key employees and/or designates to implement the emergency preparedness plan, and the organization's expected responses
- d. a notification process for stakeholders
- e. training for employees and other stakeholders as appropriate
- f. regular review and update of the business continuity plan

7.3

Policies, procedures, or guidelines describe how the organization will respond when contacted by the media, including:

- a. answering initial inquiries
- b. identifying a spokesperson/who to contact
- c. protecting the privacy of service users
- d. protecting the reputation of the organization

7.4

Policies and procedures demonstrate the organization's commitment to compliance with all legislation, regulation, and requirements, and include at minimum:

- a. a designated employee who is responsible for ensuring that the organization is in compliance
- b. that the board of directors is provided written assurance of compliance from the ED/CEO on a regular basis

7.5

Policies and procedures outline, at a minimum:

- a. what litigation matters needs to be documented
- b. what action steps are to be taken
- c. whom litigation matters need to be shared with

7.6

Policies and procedures ensure:

- a. that all contractors/consultants have appropriate coverage as required, and documentation of this coverage is obtained by the organization
- b. that a formal agreement exists between the contractor/consultant and the organization
- c. that all work or services that the organization purchases are monitored and evaluated to ensure compliance with the formal agreement and satisfaction with work or services provided

7.7

The organization ensures that appropriate types and levels of insurance coverage are in place for the protection of the entire organization and:

- a. coverage is reviewed regularly with an insurance broker or company
- b. the board of directors is informed in writing of the adequacy of the coverage

7.8

A sampling of records and/or files of service users, employees, and volunteers are monitored and reviewed regularly to ensure that they are kept in accordance with policies, procedures, and regulatory requirements.

7.9

Policies and procedures describe how the organization identifies, responds to, reports, and reviews serious occurrences and/or reportable events.

7.10

Policies and procedures describe how the organization responds to formal and informal complaints, criticisms, and suggestions for improvements from all stakeholders, and include:

- a. providing information for making, reporting, responding to, and resolving complaints
- b. ensuring a non-reprisal approach
- c. ensuring a non-retaliatory approach

7.11

Policies and procedures address how employees and volunteers ethically and responsibly use the internet, and include directives for:

- a. non-work-related internet use, social networking sites, and email
- b. protecting the privacy of service users on social media
- c. protecting the reputation of the organization on social media

7.12

An information technology (IT) plan is developed and regularly reviewed to assess the organization's day-to-day operations and guide the future IT environment. The plan includes, at minimum:

- a. physical security of technology
- b. password protection
- c. third party and remote access
- d. anti-virus protection
- e. firewall and intrusion monitoring
- f. portable data-storage devices
- g. inventory and licences of hardware and software

- h. system maintenance
- i. IT disaster-recovery process
- j. person(s) responsible for executing the components of the plan

7.13

The information technology (IT) plan is available on site at the organization and a minimum of two designated people within the organization are aware of the location and contents of the information technology (IT) plan.

7.14

All organizational policies and procedures are reviewed no less than every five years to ensure relevancy and accuracy.

7.15

The organization considers risks associated with accepting non-monetary donations, and outlines the acceptance, distribution, and storage processes.