

§ 143B-1331. Business continuity planning.

The State CIO shall oversee the manner and means by which information technology business and disaster recovery plans for the State agencies are created, reviewed, and updated. Each State agency shall establish a disaster recovery planning team to work with the Department, or other resources designated by the State CIO, to develop the disaster recovery plan and to administer implementation of the plan. In developing the plan, all of the following shall be completed:

- (1) Consider the organizational, managerial, and technical environments in which the disaster recovery plan must be implemented.
- (2) Assess the types and likely parameters of disasters most likely to occur and the resultant impacts on the agency's ability to perform its mission.
- (3) List protective measures to be implemented in anticipation of a natural or man-made disaster.
- (4) Determine whether the plan is adequate to address information technology security incidents.

Each State agency shall submit its disaster recovery plan to the State CIO on an annual basis and as otherwise requested by the State CIO. (2015-241, s. 7A.2(b).)