Axiom Business Continuity and Disaster Recovery
Dated: May 1, 2018

Business Continuity Plan (BCP)

Key personnel and vendor outside contact information shall be maintained in the Axiom Business Continuity Contact List document with periodic review and updates as needed.

The password safe(s) or equivalent as needed for administration and recovery host or server access shall be maintained and periodically updated for BCP purposes.

Offline backups of production services and data shall be maintained with all necessary data and keys for backup decryption maintained and updated for BCP contingency use.

Axiom (a Gentech, LLC proprietary software package ("Gentech")) maintains operations at two locations such that if either location should be disrupted in a non-transient manner, partial or complete service can be restored at the other location through manual or automated intervention within 24 hours within most foreseeable circumstances with the intervention of Axiom/GenTech employees in key roles and the assistance of Axiom/Gentech service providers, such as telecom services.

High-risk or high-impact areas of concern to business continuity will be assessed in the Risk Assessment program. Axiom/Gentech shall develop and maintain written contingency plans for contingencies identified as reasonably foreseeable by the Risk Assessment program.

Risk Assessment Policy

Risk assessments to areas that impact business continuity shall be periodically performed or reviewed on at least an annual basis, modeled or based on NIST SP 800-30 r1 risk assessment standards.

Business Impact Analysis

Impacts on business should disaster occur shall be reviewed/updated periodically on at least an annual basis.

Recovery Capability

Recovery capability and BCP will be tested and verified no less than annually.

In a business continuity scenario, Axiom/Gentech intends to have restored most disrupted systems within 24 hours, and all within seven days.

When operating in recovery mode, Axiom/Gentech will remain compliant with all IS Policy and agreements regarding privileged data.