DATA DRIVEN SAFETY, LLC ("Company")

Information Technology Security Policy

POLICY STATEMENT

It is a chief responsibility of the Company's Chief Technology Officer and his/her staff (the "IT Department") to continually and without interruption provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely. This mandate is designed to ensure the security, safekeeping, proper use and integrity of all data and configuration controls. This can only be accomplished by maintaining an environment designed to provide continued availability of data and programs at all times to (and only to) Company's authorized employees.

Summary of Main Security Policies.

1. Confidentiality of all data is to be maintained through discretionary and mandatory access controls that shall be reviewed on an annual basis by the DDS Executive Team. These access controls shall be designed and thoughtfully implemented so that they at all times meet or exceed industry standards for data aggregation firms operating in the United States. The efficacy of such controls shall be reviewed by the IT Department on at least a weekly basis.

2. Internet and other external service access shall remain restricted to authorized DDS personnel only. Updates to a listing of authorized DDS personnel shall be made within one (1) business day of a change event that adversely impacts the rights of such personnel to access relevant services (e.g., termination, re-assignment, etc.). Determination of proper access shall be made by the HR function and subject to the decision of the DDS Executive Team.

3. Access to data on all laptop computers shall continue to be secured through full disk encryption and other means so that confidentiality of applicable data is protected in the event of loss or theft of equipment.

4. Only software authorized by the IT Department may be installed on any DDS system, and installation of such may only be performed by the IT Department staff. Processes shall be maintained to ensure DDS personnel's compliance with this requirement. In the event of unauthorized software being discovered it will be removed from the workstation (or other hardware device) immediately and appropriate remedial action will be taken by the Company in response to the policy violation.

5. Data may only be transferred (either internally or externally) for lawful purposes and in accordance with all legal obligations imposed on DDS. Each such transfer shall be made in a manner thoughtfully and reasonably designed to safeguard the data from unauthorized disclosure or misuse. Data shall be transferred with such timing and in such manner as may be approved by the IT Department in accordance with the direction of the DDS Executive Team. Data transfers containing personal information shall be logged. Bulk data transfers shall at all times require passkey authentication by a member of the Executive Team and shall be subject to full logging.

6. All diskette drives and removable media from external sources shall be virus checked before they are used

within the Company. DDS Personnel shall employ data blockers whenever connecting to external power supplies via USB.

7. Passwords must be unique, changed at an interval consistent with industry expectations. In addition, all passwords shall consist of a mixture of at least 10 alphanumeric characters and symbols. No passwords shall be stored in writing at DDS or near DDS equipment. Password management tools shall be used in accordance with periodic IT Department mandates.

8. The physical security of computer equipment will conform to recognized loss prevention guidelines. To that end, workstation configurations may only be changed by IT Department staff.

9. To prevent the loss of data, the IT Department shall ensure a properly functioning back-up system that is geographically redundant and comprised of bare metal servers with full disc encryption that are synced with production systems within industry-accepted timelines. A business continuity plan will be developed and tested on a regular basis.

10. This Policy shall be reviewed by the DDS Executive Team at least once per year.