Predibase Data Security Schedule

1. Organizational management and dedicated staff responsible for the development, implementation and maintenance of the Predibase's information security program.

2. Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Predibase's organization, monitoring and maintaining compliance with the Predibase's policies and procedures and reporting the condition of its information security and compliance to internal senior management.

3. Data security controls which include, at a minimum, logical segregation of data, restricted (e.g. role-based) access and monitoring, and utilization of commercially available industry standard encryption technologies for Personal Data that is transmitted over public networks (i.e. the Internet) or when transmitted wirelessly or at rest.

4. Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g. granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking access promptly when employment terminates.

5. Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords.

6. System audit or event logging and related monitoring procedures to proactively record user access and system activity.

7. Physical and environmental security of data centers, and server room facilities containing Personal Data designed to: (i) protect information assets from unauthorized physical access, (ii) manage, monitor and log movement of persons into and out of the Predibase's facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.

8. Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems, including secure disposal of information or data.

9. Change management procedures and tracking mechanisms designed to test, approve and monitor all material changes to the Predibase's technology and information assets.

10. Incident management procedures design to allow Predibase to investigate, respond to, mitigate and notify of events related to the Predibase's technology and information assets.

11. Network security controls that provide for the use of enterprise firewalls, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.

12. Vulnerability assessment, patch management and threat protection technologies, and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.

13. Business resiliency/continuity and disaster recovery plans designed to maintain service and/or recovery from foreseeable emergencies or disasters.