EXHIBIT C

HD Supply Support Services, Inc.

Information Protection Policies

HDS vigorously protects its hardware, software, systems and networks, and the confidential and proprietary information stored, transmitted or manipulated by each. HDS systems are to be used only for the business purposes of HDS. HDS may periodically monitor, and/or review after the fact, the use of its Systems, Information and any other technology owned, licensed or leased by HDS. The requirements set forth in this Exhibit may be modified by HDS at any time with thirty (30) days prior written notice to Vendor provided that Vendor's written approval has been obtained.

Any capitalized term not defined in this Exhibit shall have the meaning given to such term in the Agreement.

General Policies and Procedures

1. It is the responsibility of Vendor and its employees to conduct their business with HDS in a legal and ethical manner. Vendor will maintain and enforce security policies that, at a minimum, comply with relevant industry standards and protect the integrity of HDS' technology resources and the confidentiality of HDS' Information.

2. HDS requires the name and contact telephone number of each individual authorized to access the System.

3. Passwords must be manually entered in order to log onto the System and the password must comply with HDS Password policy. Please request additional details if you are unfamiliar with the requirements.

4. A password will be known only to the user and the HDS System Administrator. There shall be no sharing of passwords except in an emergency.

5. A compromised password, (e.g., a password that has become known to anyone else at any time, including in an emergency) is not to be reused.

6. All access to the System must originate from within the United States unless approved in writing by HDS' Chief Information Security Officer.

7. Anyone who has been convicted of any felony, or a misdemeanor offense related to computer security, will not be allowed to serve as an authorized user for access to the System.

8. Vendor employees may not transfer personal or Vendor data files or software to the System, including software that is in the public domain (e.g., shareware or freeware), without prior written consent from HDS' Chief Information Security Officer.

9. Vendor employees may not transfer HDS data files or software from the System to any personal or Vendor systems.

10. If Vendor employee discovers a virus that may affect the System, s/he must report it immediately to HDS' Chief Information Security Officer at infosec@hdsupply.com.

11. Vendor employees using or creating HDS Information, or the proprietary information of others, in the course of their work with HDS, will ensure that such information is properly marked, transmitted and stored in order to ensure that the Information will continue to remain confidential and proprietary.

12. Knowledge gained about HDS, its work, vendors, plans, procedures, and etc., while providing services to HDS will not be used for personal gain or for the gain of other persons, companies, organizations or governments.

13. Any HDS equipment used by Vendor must be immediately returned to HDS upon request or if the TAA has been terminated for any reason.

14. Vendor agrees to use only remote access software that is approved in advance by HDS.

15. Vendor will promptly notify HDS upon termination of employment or reassignment of Consultant with remote or on-site access to the System so that user IDs may be changed or deleted and other necessary preventive measures may be taken by HDS to prevent unauthorized access.