Information Technology Group
Policy Name: Desktop Backup and Collaboration Tools
Date Issued: 05/02/2013

1. Introduction
   ITG staff manages computer system file and data backups for faculty and staff at the Columbia Business School (CBS). ITG also selects the software and tools used to perform the backups and collaboration services.

2. Audience and Scope
   This policy is applicable to all faculty and staff of Columbia Business School that use CBS owned and managed systems.

3. Purpose
   The purpose of this document is to set policy for CBS Faculty and Staff policy with respect to data backup and collaboration services and clarify ownership of, and access to, data that resides on these machines. The policy is intended to prevent information loss, inadvertent or deliberate data destruction, and to protect CBS data in the event of a computer theft.

4. Compliance and Regulatory Statement:
   a. Confidential data should never be stored on CBS backup or collaboration tools. See the Data Classification Policy* for more information.

5. CBS community member (faculty and staff) responsibilities:
   a. Backup
      i. The end-user is responsible for ensuring that their machine is fully backed-up after the successful installation of the backup software agent by ITG personnel.
      ii. The end-user is responsible for ensuring that the data being backed-up does not violate policy as outlined in the data classification policy*.
   b. Collaboration Tools
      i. End-users may select to utilize one of the ITG selected collaboration tools, these tools are expressly intended to synchronize data across multiple systems to aid in research and collaboration with internal and external community members and business partners.
      ii. The end-user is wholly responsible for the content and control of all data disseminated to community members and business partners utilizing the tools provided by ITG. Copyrighted and classified data must never be shared or distributed with these collaboration tools.
      iii. Data identified as containing PII or under contract such as Non-disclosure must not be stored or transmitted using these tools.

6. Security
   a. Information stored in backup and collaboration services must be encrypted in transit with at least 2048-bit transport-layer security.

b. Storage must be encrypted at rest with at least AES 256-bit encryption.

7. Data Ownership and Access
    a. There shall be a presumption that all data stored on Columbia-owned computers shall be the property of Columbia University.
    b. For administrative purpose, select ITG staff may:
        i. Access information contained in end-users backup and/or collaboration tools account. This access must be authorized by the Office of General Counsel, Human Resources, or Police subpoena.
        ii. Control how your backup and/or collaboration tools account(s) may be accessed or deleted.
        iii. Access the information files, without looking at the content, for system configuration purposes or at the request of the end users.

8. Retention
    a. Columbia Business School will retain data stored in client backup and/or collaboration tools for no longer than a 90-day period after termination of employment.
    b. Access to data backups after the date of termination is only available with written approval from Columbia Office of General Counsel or Human Resources.
        i. Managers, in cooperation with end-users should review and transfer data before employee leaves so that authorization from OCG/HR does not hold up transition.
    c. Accounts are non-transferable.

Revision History:

Version	Author	Date	Comments
.9	Ryan Whitworth	04/12/2013	Draft Document
.91	Eric Hall	04/18/2013	Minor changes to section 4, 7, 8
1.0	Ryan Whitworth	05/02/2013	Final Draft