Security Measures to Protect and Back Up Data

All data relevant to the administration of the College, including all student records, are protected in multiple ways. Specifically, electronic data stored on College servers is protected 1) from outright theft due to an intrusion into College networks, 2) from disclosure to unauthorized parties in violation of privacy and use policies, and 3) from accidental loss of any kind.

Measures to Secure Data By Defending Against Intrusion into College networks

A number of countermeasures are in place to mitigate risk from possible network intrusions and data breaches:

- The external edge of the Davidson network is protected by an intrusion prevention system (IPS) and a number of firewall layers.
- In addition, our Internet Service Provider (ISP) maintains their own perimeter security systems and firewalls (see www.mcnc.org for further information about our internet provider and its services).
- When communicating with off-premise cloud solutions, all access is controlled by authentication that occurs locally within our network via Davidson’s single sign-on protocols. User names and passwords are not exposed to the open internet. All other data passing between a Davidson user and a remote application is fully encrypted using high-bit SSL (single-socket layer) encryption. Cloud service vendors must specify by contract how they protect their own environments from intrusion or data loss and the College scrutinizes those contracts prior to utilizing the vendor’s services to insure minimum standards of security will be maintained.

Security Breaches

In the event that, despite all precautions, a data breach occurs and is recognized, the Davidson College network team will immediately:

1. Notify the Director of Systems and Networks and the Chief Information Officer of the breach.
2. Determine as nearly as possible the scope of the breach and take all measures to discontinue use of and isolate the service or system compromised.
3. Notify the Department of Public Safety who would then begin a liaison process with other law enforcement entities to investigate all circumstances related to the security breach.

Measures to Protect the Confidentiality of Data

Even those with valid credentials to gain access to Davidson networks must demonstrate legitimate need before being granted further access to administrative data. The College must comply with a number of regulatory schemes (FERPA, HIPPA, etc.) that by law protect data from general disclosure. Confidentiality of data is protected in two ways:

1. The application of fine-grained access controls at the software application and database levels for different classes of “legal” users related to their specific job roles. For example, access to different functions within Banner are controlled by Security Classes configured within the application by systems administrators. (System administrators can only grant access after seeking approval from the user’s manager and/or a data custodian who
2. Log in passwords must also be changed at regular intervals and conform to a minimum level of complexity.

Both of these topics are discussed further in the separate document titled *Davidson College Administrative Data Security Policy*.

### Measures to Protect Data from Accidental Destruction

A number of measures are in place to provide backup and recovery of data as protection against its accidental corruption or destruction due to hardware failures, software failures, inadvertent human errors, or environmental disasters.

1. All data files, document files, and system configurations that are stored on College servers and deemed to be significant, including all student records, are backed up daily and at other intervals as well depending on the exact type of data and its volatility.

2. The College employs NetBackup, an enterprise-level backup and recovery application to automate the backup processes and, if needed, to manage the recovery of data from the backups. Automation of these procedures produces highly consistent results and eliminates common human errors in performing backups and recoveries manually.

3. All backups are created and stored on disk arrays at a remote data center in an off-campus location and are therefore physically separated from the production systems being backed up.

4. Backups are retained depending on the type of data. Retention periods range from seven days to as much as twelve months. Retention schedules are created and maintained in NetBackup as “policies” which the system will execute automatically.

5. Application databases are backed up on a daily basis and in multiple ways. For example, the database for the College’s core ERP system (Banner) resides in an Oracle database. Offline backups of the database files are created each night as well as a full online export of all database objects. The offline backups paired with real-time transaction logs allow full recovery of the database to a specific point in time. The exported objects, on the other hand, permit finer-grained recovery of even a single table if there is accidental corruption. Further, updates to the Banner database are replicated in near real time to a standby database at a remote off-campus data center. This will minimize downtime in any of a number of disaster scenarios. Similarly, all SQL Server databases are backed up on a daily basis using the appropriate vendor-provided tools to automate the process.

6. All college-managed workstations and laptops are configured with the CrashPlan backup tool which backs up data continuously throughout the day in real time. This backup data is also stored at an off-site location. Missing or corrupted files can be quickly restored from backup using this tool.