## Contents

### I System Configuration and Policies

- 0.1 Access from the Network .......................................................... 4
- 0.2 User Access ................................................................................. 4
  - 0.2.1 Requesting and Granting User Access .................................... 4
  - 0.2.2 Creating User Accounts on the System ................................. 4
    - 0.2.2.1 Default Access Guidelines ............................................ 4
    - 0.2.2.2 User Names ................................................................. 4
    - 0.2.2.3 IIPS ............................................................................ 5
    - 0.2.2.4 Colleague .................................................................... 5
  - 0.2.3 User Orientation .................................................................... 5
- 0.3 Security ....................................................................................... 6
  - 0.3.1 Passwords ............................................................................ 6
  - 0.3.2 Additional Access Control .................................................... 6
  - 0.3.3 System Auditing .................................................................... 6
- 0.4 File and Directory Permissions ................................................... 6
  - 0.4.1 Exceptions ............................................................................ 6
    - 0.4.1.1 TDClient ...................................................................... 6

### II System Maintenance and Upkeep

- 0.5 Weekly System Maintenance ....................................................... 8
  - 0.5.1 Schedule .............................................................................. 8
  - 0.5.2 Notification .......................................................................... 8
  - 0.5.3 Collage: Database Maintenance ........................................... 8
    - 0.5.3.1 Backup ......................................................................... 8
    - 0.5.3.2 File Maintenance ............................................................ 8
    - 0.5.3.3 Loading Collage Patches ................................................. 8
  - 0.5.4 IIPS: Database Maintenance .................................................. 8
  - 0.5.5 OS Maintenance ................................................................... 8
    - 0.5.5.1 System Backup .............................................................. 8
    - 0.5.5.2 Solaris Patches ............................................................... 9
    - 0.5.5.3 Removing a Bad Patch .................................................... 9

### III System Backup

- 0.6 Backup Schedules ...................................................................... 11
  - 0.6.1 Daily .................................................................................... 11
  - 0.6.2 Wednesday .......................................................................... 11
  - 0.6.3 Quarterly .............................................................................. 12
  - 0.6.4 Rotating The Tapes ............................................................... 12
  - 0.6.5 Restarting the Backup Server ............................................... 12
IV Automated Processes  
  0.7 IIPS: Matrix Document Imaging ............................................. 14  
  0.8 IIPS: Campus Cruiser ............................................................ 14  

V Common Solutions  
  0.9 IIPS: No Amount On Account Receivable Receipt ......................... 16  
  0.10 IIPS: Changing Financial Aid Posting Flag ............................. 16  
  0.11 IIPS: TOADS Command Reference ......................................... 17  
  0.12 IIPS: Installing An IIPS Service Call .................................... 17  

Revisions  
Sept. 21, 2005 - Jakim Friant - Renamed section 0.2.2. Updated section 0.2.2.1 to include SSH access. Content under Security changed to a subsection labeled additional access control, and the password subsection moved under security. Added section 0.3.3 on system auditing and log files.
Part I

System Configuration and Policies
0.1 Access from the Network

The administrative unix servers for Colleague and IIPS are connected to the admin network and protected from outside access by the admin firewall. Access is only allowed from the admin network except for the following:

- Dial-up access for the following users only:
  1. VP of Student Development
  2. VP of Business Services
  3. Director of Computer Services
  4. Unix System Administrator
  5. Network Administrator

- Restricted access from specific IP addresses allowed through a NAT hole in the firewall. Currently allowing access from Wayne, the System Office, and ACS. Used for training and tech support from NCCCS.

0.2 User Access

0.2.1 Requesting and Granting User Access

User access must be requested by an employee’s supervisor. All access requests must be submitted through the Network Account Request form on the intranet\(^1\) to be approved by the Director of Computer Services. Once the request has been approved the System Administrator will fill out a User Authorization Form for the appropriate system and make sure the appropriate data owners\(^2\) have signed off on the request. Then user account will be created and the user will be notified that they must make an appointment with the System Administrator for a short orientation session to receive their username and password.

0.2.2 Creating User Accounts on the System

0.2.2.1 Default Access Guidelines

1. Telnet - All users will have telnet access to the servers from the admin network only (with the exceptions listed in 0.1).

2. FTP - Only users who have been approved for access to FTP on the User Access Form will be allowed. All others will be added to the /etc/ftpusers file to block their access.

3. SSH - System Administrators have secure shell access to perform privilege duties in an encrypted environment.

0.2.2.2 User Names

User names will be made up of the user’s first initial and the first seven characters of the last name. Any duplication issues will be handled on a case by case basis.

\(^1\)Network Account Request Form [http://intranet/forms/newfac.htm](http://intranet/forms/newfac.htm)

\(^2\)A data owner is the one responsible for fixing the data when it has been corrupted or destroyed.
0.2.2.3  IPS

Two scripts have been written to automate much of the work done to create a user. Both are in /usr/local/bin.

- `usernew` - to add users to the system
- `userrm` - to remove users from the system

When a user is added with these scripts a login "cheat sheet" will be printed that has their username and passwords.

The TOADS user name and password is in caps. Staff uses the full name separated by a period, the faculty have the first initial and first six/seven characters of the last name (like the login). All users (except for the Advisors, see below) are part of the MAIN.MENU group.

For Faculty Advisors, the TOADS Group is normally set to CFCC.ADVISOR (or CFCC.SEC for secretaries) who need to have the ability to register students. If they are going to be working in the advising center, then change the Group to CFCC.ADCNTR. The registration menu is usually "turned off" 7:00 PM on the In Service day.

Advisors are not allowed to the colon prompt.

0.2.2.4  Colleague

The user must be in the payroll system first (PERSON file), then the System Administrator can create the OPERS and SVM records for the user.

The supervisor and VP must sign off on the user access form. The VP of Business Services must sign off on all users added in collive.

1. Create the user at the unix level with: `/usr/local/sbin/setupuser`

2. First for COLTEST

   (a) Create the user in colleague with SOD in UT, following the Security Access Form for the correct security classes.

   (b) Create the user in SVM in CORE, enter the appropriate office codes from the Access Form. Note that if the user is a new employee, their record will not be in the person file so you will have to create a record from the BIO screen: first and last name is all that is necessary, and use the colleges address on ADR.

   (c) From the colon prompt, copy the user's OPERS record with the CP.OPERS paragraph. The record will be automatically copied to COLCONV, but you will be prompted about copying it to COLLIVE (in case the user had already been set up in the live account).

3. Then in COLLIVE

   (a) When the user has completed training (see below), remove the Envision password from the SOD screen.

   (b) Create the user's Staff Record with SVM. Enter same Office codes as for COLTEST.

0.2.3  User Orientation

At the beginning of the orientation session the user will be handed the Computer Services Policy to read and sign. Then the System Administrator will give a short explanation of the system and guidelines for use. The user will be told how to log in and how to change their password. Guidelines for picking a secure password and for keeping the password secret should be explained to the new user. The System Administrator will walk the user through the first log-in to make sure the user understands the procedure and to answer any questions.
0.3 Security

0.3.1 Passwords

Passwords are lower case, must be between six and eight characters long, and must contain at least two letters and one number. Passwords should not be something that is easily guessed (ex. childrens' names, spouse's name, pets).

Passwords will expire every 90 days.

Passwords must not be shared with anyone, and if written down, must be kept in a secure place (ex. wallet or purse) and must not be left on the desk or posted on the monitor.

0.3.2 Additional Access Control

On the Datatel server the system security is managed at the application level in Colleague with the use of security classes that restrict access to mnemonics, office codes that allow access to certain documents in the Communication Management modules, and a few record-level security subroutines that restrict access to individual fields and/or records.

0.3.3 System Auditing

Log files are created by the system at the OS level and reviewed daily by the System Administrators. The basic log files (/var/adm/messages, /var/adm/syslog, /var/adm/lastlog) are automatically filtered and printed daily to be kept for a year. Additional log files (/var/adm/authlog, /var/adm/maillog) are filtered and emailed to the system administrators for inspection, but a hard copy is not kept.

The Colleague application creates a log of each batch process that is run on the system that can be viewed by UTRR. While not checked on a regular basis, these can be a useful tool to find out when a process was executed and by whom.

0.4 File and Directory Permissions

The default umask on the Datatel server is 07 for users and 0022 for root, which means files normally are created as 770 by users and 755 by root. Since all users on the system are in the group “users,” it means that every user on the system can read and modify files created by other users. Files created by root can only be modified by root, but can be read and executed by anyone.

RISK ACCEPTED: the Datatel Colleague software requires that all users be able to modify files at the operating system level. Application level security restricts what users can have access to (see security in section 0.3.2).

0.4.1 Exceptions

0.4.1.1 TDClient

Directory: /datatel/release/LIVE17/TDClient

All files created in this directory were installed by a Datatel Install Shield and have the permissions of 777. The files must stay world writable for the program to function correctly.
Part II

System Maintenance and Upkeep
0.5 Weekly System Maintenance

0.5.1 Schedule
Weekly maintenance is scheduled for 6:00 PM to 8:00 PM every Wednesday night, except for when the user schedules require the use of the system (Ex: during registration, year-end processing, etc.).

0.5.2 Notification
An email will be sent out Wednesday morning to all the users with accounts on the Colleague server to remind them to log off of the Datatel UI client before 6:00 PM.

0.5.3 Colleague: Database Maintenance

0.5.3.1 Backup
Before running the database maintenance a backup must be made of the application data. This can be accomplished by copying the remote account to the vol1 partition.

Ex: `cp -R -p /datatel/work/coltest /vol1/backup/coltest`

Update: You should use the script written for this purpose: `/usr/local/bin/colbackup`

0.5.3.2 File Maintenance
Weekly file maintenance is necessary for the UniData files used by the Colleague system. Every night the WEEKLY.UDT.FILE.ANALYSIS (WUFA) process runs to calculate the new blocksizes and modulos for each file and creates a DATATEL.RESIZE.FILES paragraph. Once a week the DATATEL.RESIZE.FILES paragraph will be run to resize the files.

0.5.3.3 Loading Colleague Patches
Colleague patches will often need to be loaded once a week, especially while the CIS project implementation is still going on. Patches are first tested by the System Office in Raleigh before being released to the beta test colleges. Once we receive a new set of patches they will be loaded in the Test account first.

Patches should be loaded in the Test account when they are first released and the users will be notified of what patches have been loaded and the documentation that accompanied the patches.

Patches should be tested for at least one week before being loaded in the Live account. User sign-off must be gotten before loading any HR or CF patch that affects the payroll staff.

0.5.4 IIPS: Database Maintenance
Once a week the system log in CC.RG must be purged. Normally this is done on Friday.

Ex:
```
LOGTO CC.RG
CLEAR.FILE SYS_LOG
```

0.5.5 OS Maintenance

0.5.5.1 System Backup
As long as a good system backup was made the night before no additional backups are needed before performing system maintenance Wednesday night. The caveat is that if there has been significant data entry during the day, for example during registration, it may be wise to make a full system backup before performing any significant OS maintenance.
0.5.5.2 Solaris Patches

Once a month the SunSolve Patch Support Portal website\(^3\) should be checked for new patches. This can be done by downloading the patchdiag.xref file and uploading it to the directory where the patch check script (pca) is stored and then by running the patch check script to see which patches the system needs.

Because we do not have a duplicate server for either admin system care must be taken to determine the effects of an OS patch. Patches must be loaded with the patchadd command and the option to make a backup of the files replaced should be left on, which is the default, so that the system can be recovered if the patch causes it to crash.

Special care must be taken with kernel patches and they must be loaded individually. The system must be rebooted after each patch is loaded to make sure the kernel does not panic and render the system unusable. Any bad patch can be backed out with the recovery method detailed below.

0.5.5.3 Removing a Bad Patch

Patches added with the patchadd command can be removed from the system with the patchrm command:

1. `patchrm <patch_number>`

Patches that cause a kernel panic or other system crash require additional steps to remove. For those the system has to be booted from a CD and the filesystem mounted manually so the patch can be removed:

1. during the boot press STOP + A to get to the {ok} prompt
2. insert the Solaris 2.6 CD
3. reboot with the command boot cdrom -s, which will put you into single user mode using the kernel on the CD
4. make a directory under /tmp (ex: /tmp/work)
5. mount the partition that is normally root on to /tmp/work. Ex: `mount /dev/dsk/c0t0d0s0 /tmp/work`
6. mount all the other hd partitions in their normal places under /tmp/work. Ex: `mount /dev/dsk/c0t0d0s6 /tmp/work/usr`. This is necessary for the change root command to work below.
7. change to the /tmp/work directory (may not be necessary)
8. change the root dir so that you'll be working as if the regular file system was mounted: `chroot /tmp/work /bin/sh`
9. now you'll be able to remove the offending patch: `patchrm <patch_number>`

Note that these steps were developed for Solaris 2.6, but should work for other versions of Solaris.

Part III

System Backup
0.6 Backup Schedules

There are three different backup schedules on shamash, with specific tapes that are assigned to "pools." Each schedule has a specific frequency and retention rate.

- Daily Backup - retained for 2 weeks
- Wednesday Backup - retained for 1 month
- Quarterly Backup - retained for 1 year

It is important to note that the retention rate is based on the last backup written to the tape. So a daily backup tape that was used on December 3, 10, and 17 would retain all the backups until the last one expired on the January 1. This can cause problems with the tape filling up.

The backup tapes are organized into pools. The daily backup is actually spread across 5 individual pools to make sure that a particular week day only writes to a specific tape.

0.6.1 Daily

The daily backup has three sets of tapes (see table 1). Since there are not enough slots in the tape robot to hold all the tapes, they are rotated between the cabinet and the robot. Up to now the tapes have been rotated once a month, but since this depends on the amount of data being backed up, it may decrease. In any case, the minimum rotation time must be 3 weeks to give the old tapes time to expire so they can be re-written.

<table>
<thead>
<tr>
<th></th>
<th>Mon</th>
<th>Tue</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set 1</td>
<td>EY 1875</td>
<td>EY 1885</td>
<td>EY 1887</td>
<td>EY 1888</td>
<td>EY 1889</td>
</tr>
<tr>
<td>Set 2</td>
<td>EY 1905</td>
<td>EY 1906</td>
<td>EY 1907</td>
<td>EY 1908</td>
<td>EY 1909</td>
</tr>
<tr>
<td>Set 3</td>
<td>EY 1890</td>
<td>EY 1891</td>
<td>EY 1892</td>
<td>EY 1893</td>
<td>EY 1894</td>
</tr>
</tbody>
</table>

0.6.2 Wednesday

The Wednesday backup is a special case. It differs from the daily backup only by retention time. There are five tapes in this pool (see table 2) and once a week, one of them will be taken to our offsite location, the safe in the North Campus business office, for safe keeping. So these tapes rotate between the robot, the remote site, and the cabinet.

<table>
<thead>
<tr>
<th></th>
<th>Wed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>EY 1883</td>
</tr>
<tr>
<td>Week 2</td>
<td>EY 1886</td>
</tr>
<tr>
<td>Week 3</td>
<td>EY 1896</td>
</tr>
<tr>
<td>Week 4</td>
<td>EY 1882</td>
</tr>
<tr>
<td>Week 5</td>
<td>EY 1897</td>
</tr>
</tbody>
</table>
0.6.3 Quarterly

Finally there is a backup schedule that runs every 3 months and has a tape for each quarter (see table 3. Once this backup is completed it will be immediately taken off site to the safe deposit box at BB&T and stored there for a year. There is also a tape called the Catalog Backup that must accompany the Quarterly tape. It is assigned to the default NetBackup pool but is designated as NBBACKUP.

<table>
<thead>
<tr>
<th>Table 3: Quarterly Backup Tapes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Tape</td>
</tr>
<tr>
<td>EY 1876</td>
</tr>
<tr>
<td>Catalog Tape</td>
</tr>
</tbody>
</table>

0.6.4 Rotating The Tapes

Every so often the tapes currently in the robot will start filling up and need to be rotated out and replaced with empty tapes.

For the Wednesday backup, the tape must be taken out every Thursday and the next available tape put back in it’s place.

0.6.5 Restarting the Backup Server

If for some reason you need to restart the NetBackup server, you must be logged in as root and then execute the following commands:

```
/usr/openv/netbackup/bin/goodies/bp.kill_all
/etc/rc2.d/S77netbackup
```

That will stop the running daemons and then restart them.
Part IV

Automated Processes
0.7 IIPS: Matrix Document Imaging

The document imaging server downloads a flat file every night from the IIPS server. The file is created when cron runs the script, `/u3/admin.dev/matrix.sh`, that runs a PEXTRACT process to generate a file that contains the name, SSN, and birth date of all the students in the database. The file is created as `/u/CC.RG/EXTRACTS/MATRIX.TXT` and then is copied to `/export/home/matrix` so it can be downloaded by the matrix server.

0.8 IIPS: Campus Cruiser

A custom package has been written for exporting students to the Campus Cruiser database. Cron runs the `/u3/admin.dev/ccruiser.sh` script which in turn runs other INFO-BASIC programs to generate the files needed by Campus Cruiser. During registration this script is run twice a day, every day. At other times it is run only once a day during the work week.
Part V

Common Solutions
0.9  IIPS: No Amount On Account Receivable Receipt

Usually you’ll need to fix this problem because of a power outage that occurred while they were entering the receipt information. The problem is that the information has posted to G.L.ACTIVITY but not to AR CASH. You can check this by going to the AR CASH file and listing the receipt number. If the entry is not there, then that is what you need to add.

Note: If the account is not balancing, tell Bookkeeping to run the "Update ARMASTER" process to fix it.

Example:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Command</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>LOGTO CC.AR</td>
<td></td>
</tr>
<tr>
<td>:</td>
<td>LIST AR CASH receipt number</td>
<td>To check the entry</td>
</tr>
<tr>
<td>:</td>
<td>ED AR CASH receipt number</td>
<td>To edit the entry</td>
</tr>
</tbody>
</table>

You’ll need to add the information that is missing. The easiest way to do this is to look at another receipt that has similar information (Usually one they just entered). The important parts are the AR account, the amount, and the transaction type (cash, charge, third party account, etc.)

The fields you will need to enter are:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Term</td>
</tr>
<tr>
<td>8</td>
<td>AR CODE</td>
</tr>
<tr>
<td>9</td>
<td>Amount</td>
</tr>
<tr>
<td>10</td>
<td>Cashier’s Initials</td>
</tr>
<tr>
<td>11</td>
<td>Check Number</td>
</tr>
<tr>
<td>12</td>
<td>(Leave empty)</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
</tr>
</tbody>
</table>

0.10  IIPS: Changing Financial Aid Posting Flag

This will need to be changed if the Business Office and Financial Aid got out of sequence with each other.

Example:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Command</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>:</td>
<td>LOGTO CC.COMMON</td>
<td></td>
</tr>
<tr>
<td>:</td>
<td>ED CONTROL.POINT FINAID.POST</td>
<td>Change to the first line</td>
</tr>
<tr>
<td>:</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>:</td>
<td>R A</td>
<td>Change the “C” to an “A” so FA can post again</td>
</tr>
<tr>
<td>:</td>
<td>F I</td>
<td>Save the changes</td>
</tr>
</tbody>
</table>
0.11  IIPS: TOADS Command Reference

<table>
<thead>
<tr>
<th>Notes</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save changes made to the current record</td>
<td>S</td>
</tr>
<tr>
<td>Cancel &amp; return to ID entry without saving changes to the current record</td>
<td>XX</td>
</tr>
<tr>
<td>Quit the current process without saving changes</td>
<td>Q</td>
</tr>
<tr>
<td>Go to the first enterable item at top of page</td>
<td>T</td>
</tr>
<tr>
<td>Go to a specific window (where # is the window number)</td>
<td>WI#</td>
</tr>
<tr>
<td>Go to a specific page (where # is the page number)</td>
<td>P#</td>
</tr>
<tr>
<td>Go to a specific item number</td>
<td>#</td>
</tr>
<tr>
<td>Delete the current record (if allowed)</td>
<td>DE</td>
</tr>
<tr>
<td>See the Process HELP narrative</td>
<td>O</td>
</tr>
<tr>
<td>See a list of additional command line options</td>
<td>?</td>
</tr>
<tr>
<td>Print a hard copy of the current screen</td>
<td>H</td>
</tr>
<tr>
<td>Jump to another process</td>
<td>J</td>
</tr>
<tr>
<td>Jump to another process with key provided</td>
<td>JK</td>
</tr>
<tr>
<td>Go back one line item or one data window line</td>
<td>=</td>
</tr>
<tr>
<td>Delete current item or data window line</td>
<td>\</td>
</tr>
<tr>
<td>Go to the TOADS command line</td>
<td>,</td>
</tr>
<tr>
<td>Move to the right one field at a time</td>
<td>&lt;TAB&gt;</td>
</tr>
<tr>
<td>Move to the next window line</td>
<td>&lt;Down Arrow&gt;</td>
</tr>
</tbody>
</table>

0.12  IIPS: Installing An IIPS Service Call

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Commands/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Get to the unix prompt ($). You should be the root user (or switch with su - root)</td>
</tr>
<tr>
<td>#</td>
<td>cd /u1/CC.COMMON</td>
</tr>
<tr>
<td>ftp&gt;</td>
<td>cd pub/scp</td>
</tr>
<tr>
<td>ftp&gt;</td>
<td>bin</td>
</tr>
<tr>
<td>ftp&gt;</td>
<td>get SCP.xxxx.tar <em>(Where xxxx is the service call number. Ex SCP.2278.tar)</em></td>
</tr>
<tr>
<td>ftp&gt;</td>
<td>bye <em>(when it's finished)</em></td>
</tr>
<tr>
<td>$</td>
<td>piopen</td>
</tr>
<tr>
<td>:</td>
<td>*PACKET.UNLOAD</td>
</tr>
<tr>
<td>Srv Call:</td>
<td>SCP.2278</td>
</tr>
</tbody>
</table>

   It will run through the installation and return you to a colon prompt. As long as there are no beeps, everything installed fine. If there are beeps, scroll up on the screen to see what errors occurred. Usually it is a dictionary item or program that didn't compile and you will need to compile it manually.