Defense MD

Backup Tape Encryption for Our Self Processing Credit Union Partners

INTRODUCTION

This document describes how to use the various controls and menu options related to encryption of backup tapes via the Defense MD system.

CONTENTS

Revision date: October 28, 2016

For an updated copy of this booklet, check out the Reference Materials page of our website:
https://www.cuanswers.com/resources/doc/special-interest-publications/

INTRODUCTION

DEFENSE MD: ENCRYPTED TAPE BACKUPS FOR SELF-PROCESSORS

Do you cringe when you read news articles about a company that misplaces a data tape and now must notify their entire customer base of the potential security risk because their personal data has landed in unknown hands? Can your business afford either the risk or the expense of a similar exposure happening in your data center? How secure are your end-of-day backup tapes when they leave your building?

As self-processors, these are questions that we must continually ask ourselves, and most certainly be ready to answer when they are asked of us by members, examiners, or vendors. As a diligent CUSO partner, you have implemented secure and practical solutions to protect member data, but to what degree will they hold up? Can they go so far as protection against a disgruntled employee walking off with an unencrypted backup tape?

Member data is the lifeblood of your business, and today's marketplace requires all of us to step up to the challenge of preserving its security. As a data processor, this same challenge is magnified to the point where it became prudent to invest CUSO financial and staff resources to develop a even higher degree of data security—tape encryption with **Defense MD**.

Defense MD allows you to securely encrypt data that you are currently putting on magnetic tape.

CU*Answers has partnered with Patrick Townsend & Associates to offer their Alliance AES/400 product to our self-processing community. The heart and soul of the Alliance AES/400 solution is its use of AES (Advanced Encryption Standard). AES is an encryption method that has been selected by the National Institute of Standards and Technology (NIST) of the US government for use in private and public applications to protect sensitive information.

During our internal deployment, CU*Answers added a user-friendly wrapper around the AES/400 product to create an easy-to-use menu system, configuration options, and invaluable assistance with key management. Defense MD can even notify you when a new library has been added to your system so that its proper disposition can be defined.

Defense MD is the solution to safely and securely protecting your valuable member data and to satisfy the scrutinizing eye of auditors and examiners.

SYSTEM BACKUP AND BUSINESS RECOVERY STRATEGIES

Several credit unions have approached us recently about the possibility of transmitting daily backup files to CU*Answers in order to eliminate the daily tape cycle. While we are working toward a solution to meet these requests, there are still valid reasons for all in-house clients to strongly consider tape encryption:

- Even if you are already using or considering a high availability/data replication solution, you will always have a need for tape backups for local restore purposes.

- And what about your full system backups?
- Or your month-end CU*BASE file backups (you should have two sets – one onsite and one offsite)?

An examiner will certainly remind you that it is critical to retain a hard copy of these backup tapes for seven (7) years. Since moving data to tape is not going away totally any time soon (even after you deploy a data replication strategy), your member data will continue to be exposed to risk without a comprehensive encryption strategy like Defense MD.

COSTS

Fees for Defense MD include a one-time software and implementation services fee of $9,000 (plus applicable T&E). This cost covers a member of our iSeries team coming on-site to configure, document, and train your staff on AES/400. The second cost is a 20% Annual Maintenance Fee. This $1,800 fee will be invoiced upon installation and each subsequent anniversary.

> *If your credit union has High Availability, there may be an additional cost to purchase a second copy of the AES/400 software for your HA backup iSeries.*
>
> *All fees are subject to change. Refer to the current year's Self Processor Pricing Guide (sent to your credit union CEO annually) for updated pricing.*

GETTING STARTED

For more information or to get signed up for Defense MD services, contact **Lora Goodin (lgoodin@cuanswers.com)** or **Scott Collins (scollins@cuanswers.com)**. Following is a summary of the process:

1. A contract will be drawn up to be signed by your credit union and CU*Answers.
2. Your credit union should develop a policy and procedure for handling encryption keys and secure transport and storage of encrypted materials. **(See the Appendix for a sample policy to consider.)**
3. We will order the Alliance AES/400 software from Patrick Townsend & Associates for you.
4. A pre-site contact will be set up to discuss the timing and process for implementation for your credit union.
5. Based on your pre-site, a CU*Answers representative will take care of loading and configuring the software on your iSeries.
6. A CU*Answers representative will provide training to your staff, either in person or over the phone as desired.
7. Your Operations staff will begin following your newly established procedures for handling daily/monthly backup tapes.

CHANGES TO YOUR POLICIES AND PROCEDURES

See the Appendix on Page 20 for a sample data encryption policy. This policy can be copied and adapted for your credit union's use, with changes and additions as appropriate.

HANDLING BACKUP TAPES

The actual steps for daily and monthly processing (see Page 8) will not change much for your Operators, but the procedures for handling the backup tapes will. This is necessary to ensure that the encryption keys are kept safe and easily accessible, but NOT stored in the same location as the backup tapes themselves. After all, the data isn't secure if someone could easily steal the tapes and the secret password codes at the same time!

> *NOTE: Data is never stored encrypted on the iSeries itself; encryption occurs at the point when files are copied from disk to tape using the command on the MNOP04 Daily Processing or MNOP03 Monthly Processing menus.*

GENERATING ENCRYPTION KEYS

In a nutshell, an **encryption key** is basically a randomly-generated password that uses a complex set of characters in a long string. Each key has a **key name** that helps to identify which backup tapes were encrypted using that particular password.

You will need to have policies and procedures in place to routinely generate new encryption keys, such as on an annual basis, according to your credit union's security policies and risk assessment. Keys must be retained for as long as the backup tapes that use those keys (old tapes continue to use the old key that was in place when the tape was generated).

> *The procedure for generating keys is part of the instructions you will receive separately with the Alliance AES/400 software. You will then use a command on the Defense MD menu (page 6) to save a backup copy of the keys to be stored in a separate off-site location.*

NEW PROCEDURE FOR FULL SYSTEM SAVES

Although the menu options your Operators will use for daily and monthly backup tapes will not change with Defense MD, in order to encrypt member data as part of your periodic full system backup, a new menu option must be used on the Defense MD menu. See Page 9 for instructions.

CHANGES TO YOUR ANNUAL DISASTER PLAN TESTING

To make sure your backup tapes will be available when you need them, we recommend you set an annual schedule to test restoring data from backup tapes using the encryption keys. This can be done as part of your annual disaster recovery testing.

In addition, be sure to make a note in your disaster plan to include the AES key file in the list of data tapes you will need in the event of a disaster. In the event that a full system restore is needed, for a DR test or after an actual disaster, the following tapes will be needed:

1. Most recent full system save (includes encrypted and unencrypted tapes)
2. AES Key file
3. Most recent EOD or BOD (depending on when disaster occurred)
4. Latest EOM
5. Most recent version of any daily backups (if done)

THE DEFENSE MD MENU

When Defense MD is installed and configured on your iSeries, a new menu will be added. **This menu will only be used in a few situations:**

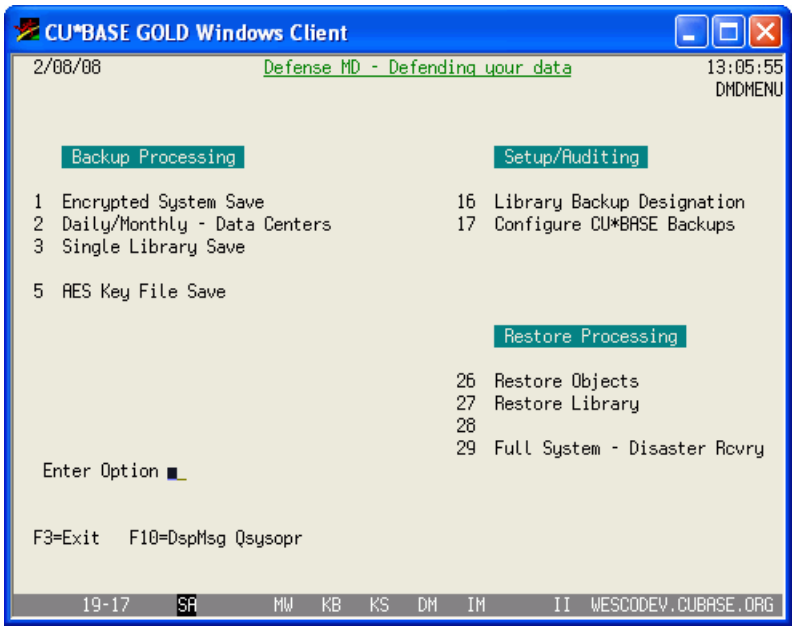
- If you need to change the configuration from what is initially set up for you by a CU*Answers representative, or
- To run your periodic full system backup (instead of using the "GO SAVE" command).
- To save or restore an individual encrypted library or file.

To access the Defense MD menu, your user profile will need to include the DEFMD library in your library list. (You may need to adjust the USERID profile for select employees who will need this library.)

From the main Operations menu MNOP01, choose option 18 "Defense MD Tools" (or type command DEFMD on a command line) to display the following menu:

The Defense MD Main Menu

MNOP01 #18 "Defense MD Tools"



Menu Options

Option	*What it does*
Backup Processing	
1 Encrypted System Save	This is the option you will use from now on to process your full system backup. **See Page 9.**
2 Daily/Monthly – Data Centers	Calls DLYMOBKCL to display the Defense MD Daily/Monthly Backups menu (Page 17). **Not used by self processing credit unions.**

Option	*What it does*
	See Page 8 for instructions.
3 Single Library Save	Calls the DMDSAVLIB command. **See Page 11.** This is used when saving a refresh of your training library or another single library in an encrypted format.
5 AES Key File Save	Prompts for a tape device and performs a SAVOBJ command. This is used to save a copy of the encryption keys to a backup tape. This tape must be stored in a secure, convenient off-site location, but NOT the same location as where the backup tapes themselves are stored.
Setup/Auditing NOTE: This area currently has only setup options but is also intended for future enhancements designed for auditing purposes.	
16 Library Backup Designation	Scans system for new libraries (UDMDLIBCL). Displays list of all libraries on system and the backup designation codes. **See Page 15.**
17 Configure CU*BASE Backups	Links to CU*BASE backup configuration program UBACUPCL. **See Page 14.**
Restore Processing	
26 Restore Objects	Calls the DMDRSTOBJ command. **See Page 12.** Can be used to restore a library, such as your end-of-month files, or even a single file.
27 Restore Library	Calls the DMDRSTLIB command. **See Page 12.** This is used to restore a fresh copy of your training library or another single library that was encrypted.
29 Full System - Disaster Rcvry	Calls the CUADRMNUCL command. **Not used by self processing credit unions.**

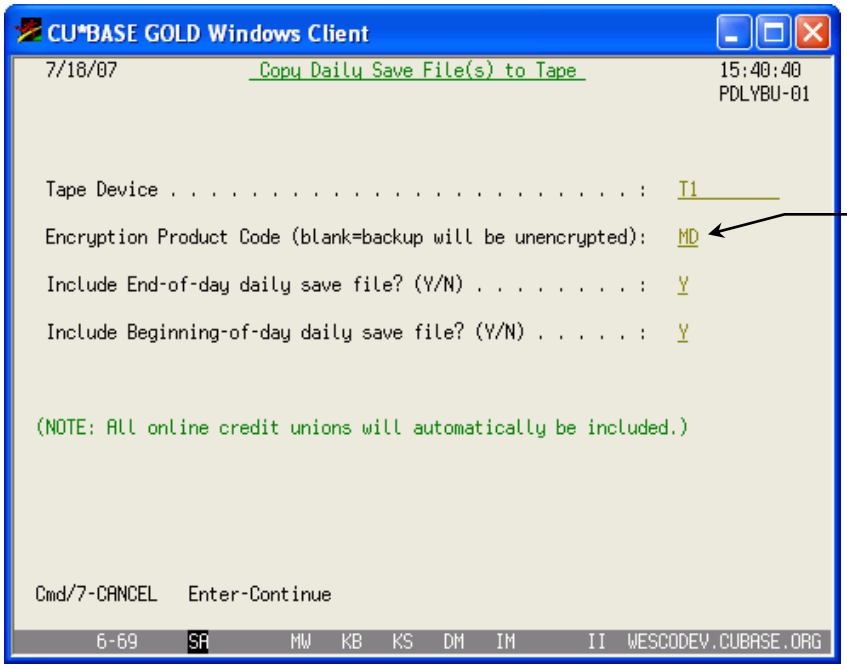
ENCRYPTING YOUR DAILY/MONTHLY BACKUPS

After Defense MD has been installed and configured on your computer, you will proceed to handle your daily and monthly processing exactly as before, using the same menu commands as usual. The main difference will occur when backups are copied to disk.

> *IMPORTANT:* ***If your credit union previously did backups directly to tape, your Operator will now need to complete an additional step*** *to select the special "copy to tape" command on either the MNOP04 Daily Processing or MNOP03 Monthly Processing menus.*

Remember that data is never stored encrypted on the iSeries itself; encryption occurs at the point when files are copied from disk to tape.

OPER #2 "Daily Processing" then #6 "Copy Daily Save Files to Tape"
(or OPER #3 "Monthly Processing" then #11 "Copy Month-End Files to Tape")



This code is pulled from the file backup configuration (see Page 14) and indicates that Defense MD is in place on your iSeries.

Because Defense MD has been configured for your credit union, this option will now automatically encrypt the data as it is copied to the tape (two copies will still be produced, as usual).

> *As with your full system backups, a printout will be produced showing the contents of the tape. (See Page 11 for a sample of this report.) We recommend that you keep the report with the tape to assist with future restores.*

YOUR FULL SYSTEM BACKUP

Use these instructions to perform a full system backup for your iSeries. (These instructions should be used instead of the "GO SAVE" command.)

IMPORTANT: When you sign in as QSECOFR to do your backup, **remember that your library list will not automatically contain the DEFMD library** needed to handle the encryption routines. Therefore, you'll need to edit your library list using the following command: ADDLIBLE LIB(DEFMD) POSITION(*LAST)

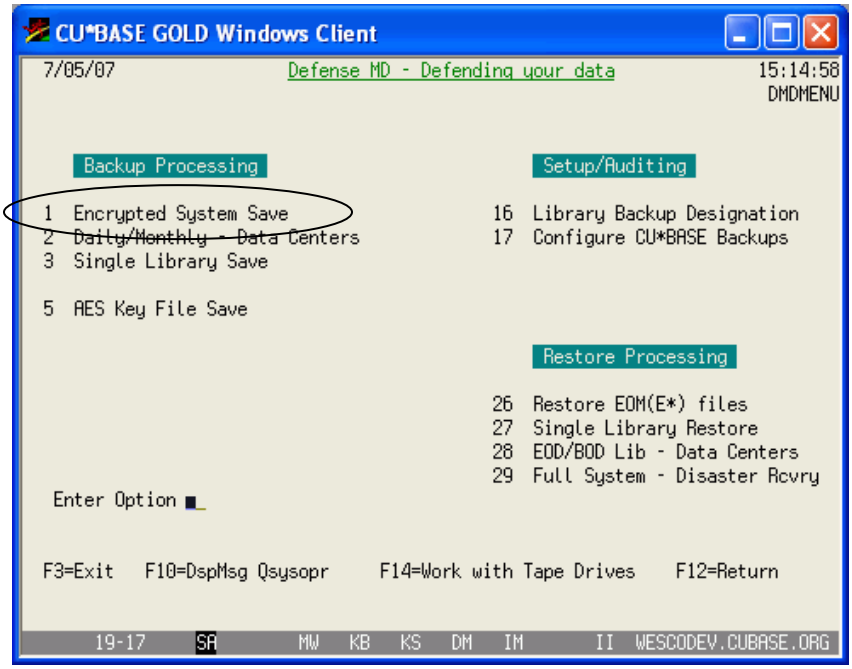
In Addition, **any 3rd party products currently running will need to be shut down** prior to starting the Defense MD Backup.

> *This includes: CUHOME, Audio Response(I3IVR), Instant Card(ICIHOST), Indirect Lending(INDIRECTL), and Near Real Time Alerts(NTALERTS)*

Please consult the following for assistance and information:

> *Credit Card/ATM Processors: Self Processor Manual/ OPER Menu*
>
> *ROBOT Scheduling Software: CU*Answers OpsEngine Department*
>
> *iTERA High Availability Software: CU*Answers iSeries Department*

Defense MD Main Menu (command DEFMD)



Use **option 1 Encrypted System Save** on the Defense MD menu to process your full system backup. (A confirmation screen with instructions will appear before continuing.)

This method uses a special configuration (see Page 15) to determine which data should be encrypted (member file libraries, employee libraries, etc.) and which can be saved without encryption (such as application files).

Two separate backup tapes will be generated. The system will instruct you when to load the first (encrypted) tape and then when to the load the second tape for unencrypted data. Following is a summary of what happens when you select this option:

1. Retrieves the device ID from DEFMD config
2. Checks for libraries designated for encrypted backups (these are configured using the screen shown on Page 15)
3. Initializes the encrypted tape
4. Saves libraries flagged for encrypted saves
5. Displays the tape to print out
6. Initializes the unencrypted tape
7. Puts system in restricted state
8. SAVSYS
9. SAVLIB *NONSYS w/ omitted libraries flagged in DEFMD config
10. SAVDLO
11. SAVE IFS
12. Displays the tape to print out and keep with the backup tapes (see Page 11)
13. IPLs the system

WORKING WITH ENCRYPTED FILE TAPES

When daily/monthly or full system backups are done as described above, the system will produce a report showing the contents of the tape:

```
5722SS7 V5R4MO 060210                TAPE VOLUME INFORMATION        TEST         TESTCOMM     7/25/07 23:32:02       Page    1

Device . . . . . :   T1                  Volume . . . . . :  TEST
Owner ID . . . . :                       Density  . . . . :  *ULTRIUM3
Type . . . . . :   *SL                   Code . . . . . :  *EBCDIC

                                Record
                    File        Block    Recg  Record  Block   File        Mvol  Mvol        Date      Expiration  System
Data File Label     Sequence    Format   Tech  Length  Length  Length      Ind   Sequence    Created   Date        Where Created

FILECLEOD           0000000001 *F       P     32736   032736  0000574523        0000000001  07/25/07  *PERM       IBM0S400
FILECLBOD           0000000002 *F       P     32736   032736  0000573426        0000000001  07/25/07  *PERM       IBMOS400
```

This report should be printed and kept with the tape itself to make it easier to see what is on the tape, and to provide the details you will need later should something need to be restored from the backup.

COMMANDS FOR SAVING & RESTORING INDIVIDUAL ENCRYPTED FILES

DMDSAVLIB Command

This command (also available via option #3 on the Defense MD menu) is used to encrypt and save a single library to tape, such as your training library.

From a command line type in the command **DMDSAVLIB** then press F4 (Prompt) and complete the fields as appropriate:

Field Name	*Description*
Library	The library that you want save.
Device	The tape drive you will be saving to.
Save file already exists?	Answer **Y** if you have already saved your library to a save file. IMPORTANT: It is recommended that the save file name you use is the same name as the library name so that the DMDRSTLIB command can be used to restore the encrypted library.
If Y, name of save file If Y, library save file in	The name and location of the file that is to be encrypted and saved to tape.

DMDRSTOBJ Command

This command (also available via option #26 on the Defense MD menu) is used to restore the E* files from End of Month backup tapes that are encrypted.

From a command line type in the command **DMDRSTOBJ** then press F4 (Prompt) and complete the fields as appropriate:

Field Name	*Description*
Device	The tape drive you will be restoring from.
Date saved	The date (mmddyy) that files were written to the backup tape. This appears as "Date Created" on the DSPTAP printout.
Save file	The name of the file, as shown under "Data File Label" on the DSPTAP printout.
Sequence number	The sequence number of the save file. This is shown under "File Sequence" on the DSPTAP printout.
Objects	The name of the objects you want to restore. ▪ For end-of-month files, use **E*** ▪ For a single file, enter the file name
Saved library	The library that the files were in when they were saved. For month-end files, use FILExx (not FILExxE).
Restore to library	The library where you want the objects restored, such as FILExxE for month-end files.

DMDRSTLIB Command

This command (also available via option #27 on the Defense MD menu) is used to restore file libraries that are encrypted, such as your training library. (If a library on the tape is unencrypted, such as CUBASE libraries, then just use the normal RSTLIB command.)

From a command line type in the command **DMDRSTLIB** then press F4 (Prompt) and complete the fields as appropriate:

Field Name	*Description*
Device	The tape drive you will be restoring from.
Date saved	The date (mmddyy) that library was written to the backup tape. This appears as "Date Created" on the DSPTAP printout.
Save file	The name of the save file, as shown under "Data File Label" on the DSPTAP printout. For an end-of-day library being restored as a new training library, the file name should be FILExxEOD.
Sequence number	The sequence number of the save file. This is shown under "File Sequence" on the DSPTAP printout.
Saved library	The library that was put to the save file. For an end-of-day library, use FILExx.
Restore to library	The name of the new library you are creating. For a training library, use FILEXX **where the XX is NOT your credit**

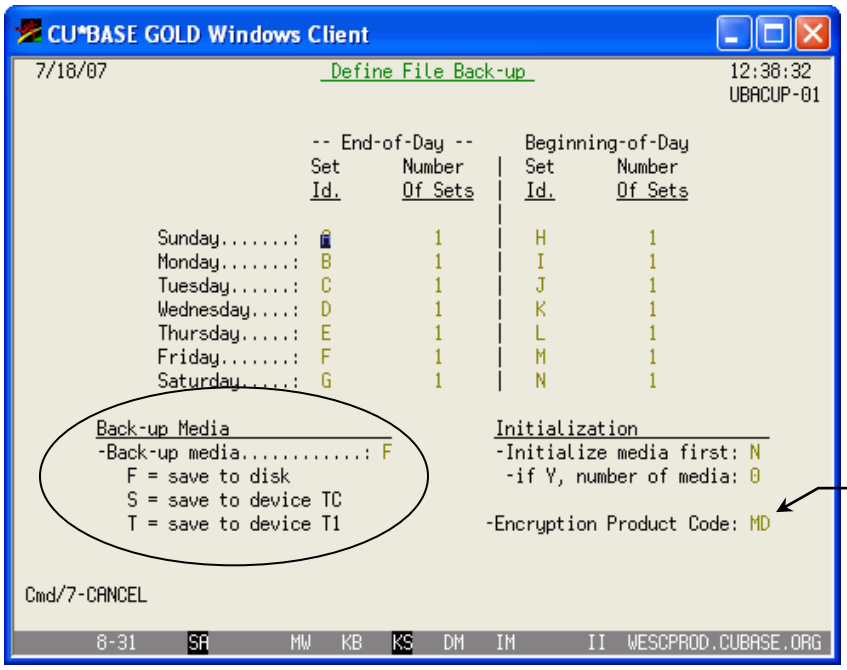
Field Name	*Description*
	union ID.

CONFIGURATION OPTIONS

IMPORTANT: The following configuration steps will be done for you as part of your initial configuration and setup for the Defense MD system. This section is presented for your information only and will generally not need to be changed unless you wish to alter which files are being included/encrypted in your full system backup.

The first step in configuring Defense MD will be to alter the way daily and monthly backups are processed.

Option 17 "Configure CU*BASE Backups" from the Defense MD menu (pg. 6)

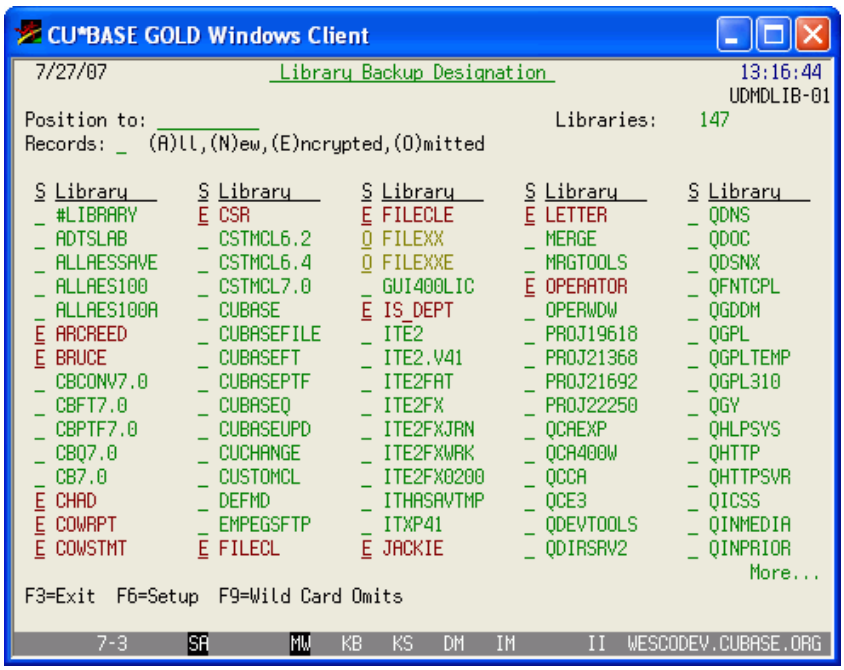


This setting will be changed to indicate that Defense MD has been loaded on your iSeries. This code will be used on the Copy Daily Save Files to Tape screen (see Page 8).

The Back-up media option must be set to "F" so that backup files are saved to disk (in your FILExxE library) rather than going directly to tape. (Your credit union may already be using this method.) An *Encryption Product Code* of MD will also be entered to indicate that the software has been set up on your iSeries.

Next, a special Defense MD configuration is used to specify how full system backups (see Page 9) will be handled. This configuration itemizes which libraries should be encrypted (your member data), and which libraries have files that can be saved in plain text, such as the libraries that contain system and application files.

Option 16 "Library Backup Designation" from the Defense MD menu (pg. 6)



The system first performs a scan (UDMDLIBCL) for any new libraries that have been added since the last time the configuration was done. The screen shows all libraries on the iSeries and any existing encryption codes you have set up.

Use the "position to" search field at the top of the screen to enter a library name and scroll quickly to that library. Or type one of the four "Records" types and press Enter to display only those libraries (clear the field or type A and press Enter to see all libraries again).

To modify the configuration, simply enter one of the following designation codes in front of the library name. When done, use Enter to save, then F3-Exit to return to the menu.

> *The decision about whether to encrypt a library or omit it from your full system backup will depend on your Disaster Recovery policy. Since your normal daily/monthly backups will be encrypted, some CUs use their full system back up to save only system files, omitting the ones that are encrypted on their regular daily backups. Then they would need both tapes (as well as the separate tape containing the encryption keys) in the event of a disaster or DR test.*

Designation Codes

Code	*Description*
E - Encrypt	Libraries marked with this code WILL be encrypted and included on the separate encrypted data tape when a full system backup is done using option #1 on the Defense MD main menu (see Page 9). > Don't forget about your QUERYxx library or any other employee libraries that might contain member data created via Query!

Code	*Description*
O - Omit	Libraries marked with this code will not be backed up at all when a full system backup is done using option #1 on the Defense MD main menu (see Page 9). Depending on your disaster recovery policy, you might use this option to omit the FILExx libraries that are already being backed up on your normal daily backups. (But if you *do* include those, make sure to encrypt them!)
N - New	All libraries that have been added since the last time this configuration was accessed will be marked with this code. These will be handled as unencrypted items (same as blank) until you change them to the desired code.
(Blank) - Unencrypted	Libraries that are not marked with any code will NOT be encrypted. They will be included on the unencrypted tape when a full system backup is done using option #1 on the Defense MD main menu (see Page 9).

Command Keys

Command Key	*Description*
F6-Setup	Used to configure some parameters used when copying encrypted files to tape, including your credit union's assigned 2 digit key ID (unique by iSeries) and default tape device. *(This setup will be done for you during your initial Defense MD installation.)* NOTE: You can also specify an email address. This is for a future enhancement planned to create a new daily job that causes the iSeries to kick out an email whenever new libraries are added. This should generally be a group email address that is monitored by more than one person.
F9-Wild Card Omits	To configure up to 10 wildcards (i.e. FILE*) for omission on the non-encrypted full system save. This feature was intended for use in service bureau situations where there are a number of libraries with similar naming convention, such as FILExx, to speed up the process of setting the designation codes.

SPECIAL NOTE TO CUS USING HIGH AVAILABILITY (HA)

If your credit union has an HA backup system for production redundancy, the Alliance AES/400 software will be loaded and configured separately for each iSeries. The software file libraries are not typically mirrored between the two systems because of the way the software is configured.

It may be appropriate, however, to mirror the DEFMD libraries that store the configuration settings above. If not, you would need to make the same changes to both IBMi systems separately, whenever new libraries are added.

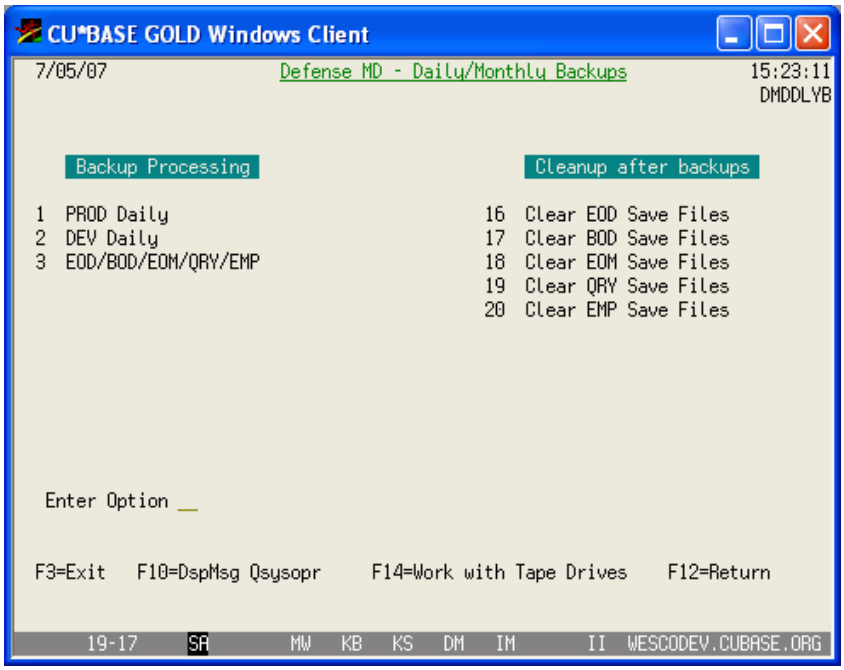
If CU*Answers acts as your HA backup system, we cannot mirror the DEFMD libraries as it would cause a conflict with our system. Therefore, we would need to coordinate changes to this configuration with you.

OTHER DEFENSE MD FEATURES

DAILY/MONTHLY BACKUPS FOR SERVICE BUREAUS

The following menu is NOT used by self processing credit unions. It was designed specifically for the special needs of CU*Answers and other service bureau environments who handle backup tasks independent of daily processing.

Option 2 "Daily/Monthly – Data Centers" from the Defense MD menu (pg. 6)



Menu Options

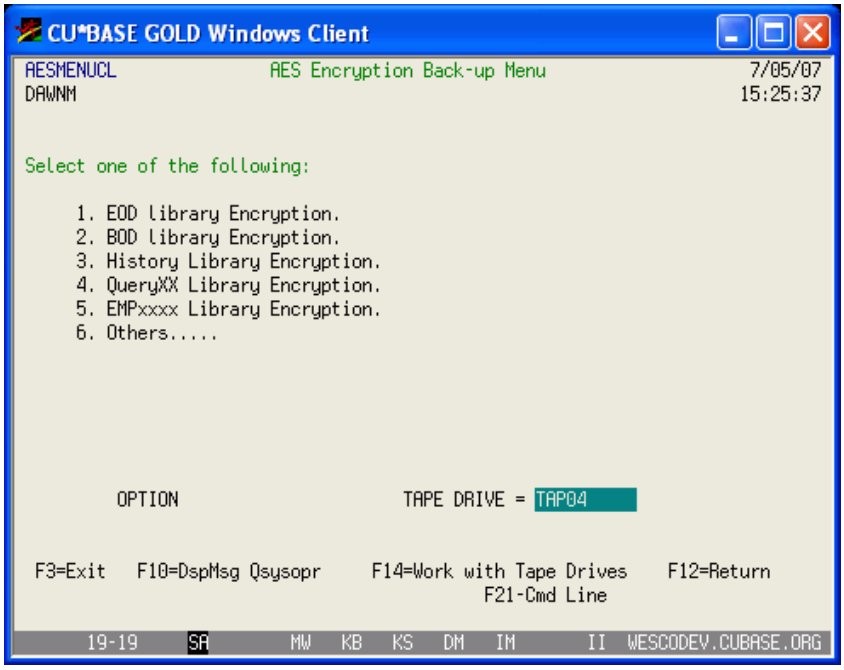
Option	*What it does*
Backup Processing	
1 PROD Daily	Calls command PRODDLY which prompts for tape device PRODDLYCL submits job PRODDLYBKP ▪ Initializes tape ▪ Encrypted backup of OPERATOR ▪ Unencrypted backup of ZMODLIB10 ▪ Displays tape to printout
2 DEV Daily	Calls command DEVDLY which prompts for tape device DEVDLYCL submits job DEVDLYBKP ▪ Initializes tape

Option	*What it does*
	▪ Encrypted backup of CNV*, EMP*, PROJ* libraries ▪ Unencrypted backup of CUBASE*, ZMODLIB10 ▪ Displays tape to printout
3 BOD/EOD/EOM/QRY/EMP	Calls AESMENUCL and displays backup options. **See Page 19.**
Cleanup After Backups	
16 Clear EOD Save Files	Calls EODSAVCLR and clears save files in the BKPEOD library.
17 Clear BOD Save Files	Calls BODSAVCLR and clears save files in the BKPBOD library.
18 Clear EOM Save Files	Calls HSTSAVCLR and clears save files in the BKPHST library.
19 Clear QRY Save Files	Calls QRYSAVCLR and clears save files in the BKPQRY library.
20 Clear EMP Save Files	Calls EMPSAVCLR and clears save files in the BKPEMP library.

AES ENCRYPTION BACKUP MENU

The following menu is NOT used by self processing credit unions. It was designed specifically for the special needs of CU*Answers and other service bureau environments who handle backup tasks independent of daily processing.

Option 3 "BOD/EOD/EOM/QRY/EMP" from the Defense MD Daily/Monthly Backups menu (pg. 17)



Each option calls AESSAVECL with the appropriate 2 parameters:

- Type of backup: B, E, H, Q, C
- Tape Device

Sets up key and save file library names. Calls corresponding CL for encryption processing:

- E – AESEODSAV
- B – AESBODSAV
- H – AESHSTSAV
- Q – AESQRYSAV
- C – AESEMPSAV

These options can be run interactively or submitted to batch.

APPENDIX

SAMPLE DATA ENCRYPTION POLICY

S A M P L E

Data Encryption Policy

Date	Revision	By

1.0 Introduction

This document describes the procedures and controls implemented by _____ (the "Credit Union") to provide protection of sensitive data by means of encryption. Encrypting sensitive data is one of the strongest ways to achieve data confidentiality and ensure protection against unauthorized or unintentional disclosure of sensitive materials.

Proper management of cryptographic keys is essential to the effective use of encryption and the ability to restore protected data in a disaster. Loss or corruption of key materials will render encrypted data unusable. Compromise of key materials may lead to compromise of encrypted data.

This document outlines what data has been determined to be sensitive, how that data will be protected (i.e. encrypted), how encrypted media is to be handled, protection and proper handling of encryption key materials, auditing responsibilities of encrypted media and key materials, who has access rights to execute encryption commands, and procedures to follow for lost or compromised encrypted data and key materials. Because much of this document addresses procedural issues, and procedures are subject to change from time to time, this document may be updated accordingly from time to time. Please be sure you are referring to the most up-to-date revision.

The document was constructed based on information contained in NIST (National Institute of Standards and Technology) Special Publications 800-57 *Recommendation for Key Management: Best Practices for Key Management Organizations*, and ISACA (Information Systems Audit and Control Association) document P9: *IS Auditing Procedure: Evaluation of Management Controls over Encryption Methodologies.*

2.0 Intended Audience and Confidentiality

The material in this document is intended for use by Credit Union management, auditing, and administrator groups responsible for implementing, auditing, handling, and operating encrypted data and/or key materials.

The contents of this document are considered confidential and may not be distributed without the written consent of Credit Union senior management.

3.0 Scope Limitations

This document is not a technical reference or encryption implementation or operational procedures guide. It also does not cover encryption policies or procedures for temporal (i.e. SSL) in-transit data encryption.

4.0 Definition of Sensitive Data

Sensitive data is data that will be protected by means of an approved data encryption algorithm implemented under the constraints of this policy.

4.1 Sensitive data is further defined as:

- Member data not generally known or available in the public domain and that is transferred electronically or physically outside of the credit union's networks or facilities

4.2 Member data not generally known or available in the public domain is further defined as:

- Social Security or other Tax ID numbers
- Account numbers
- Credit information and credit history
- Member names tied to specific institutions
- Member transactions
- Loan information

Loss of system configuration or proprietary software due to loss of a backup tape, while undesirable, is not considered a significant business risk. Such information is not considered sensitive enough to protect with encryption.

The Credit Union uses custom backup software that creates two separate backup jobs: one that contains sensitive information and a second one that does not. The sensitive data will be encrypted on the tape. Both data sets will be needed to restore a system from scratch. Both data sets may be stored on the same tape.

5.0 Risks to Sensitive Data

Unauthorized disclosure of or access to member data creates a significant risk to both the Credit Union and its members. The Credit Union has gone to great lengths to ensure network access to data is restricted by various sophisticated technical mechanisms that comply with a written Data Security Policy. Periodic independent audits on controls and processes ensure policy is being followed. Technical mechanisms are detailed in various other risk analysis and policy documents and are beyond the scope of this document.

Compromise of a backup tape with member data could have serious financial liabilities to the Credit Union and its members. Therefore it is essential that steps be taken to protect member data stored on tape through proper tape handling procedures (detailed in various SOP guides external to this document) and strong data encryption.

6.0 Approved Encryption Algorithm Protocols

The Credit Union will only approve industry-standard strong encryption algorithms. The Credit Union does not use custom or proprietary algorithms for protection of sensitive data. As a general rule of thumb, the Credit Union will use FIPS (Federal Information Processing Standard) approved algorithms for protection of sensitive data, though exceptions may be found where non-FIPS approved algorithms may be used where an algorithm has withstood extended and significant scrutiny and enjoys wide adoption in various industries.

For backups to tape, symmetrical algorithms make sense due to their ease of use and understanding over asymmetrical algorithms. Multiple keys can be created for use with trading partners. AES (Advanced Encryption Standard) encryption is very fast (as compared with 3DES) and more secure. AES is platform agnostic and can be decrypted on platforms differing from the originating host (though the decrypted data may not be compatible with a different host's file system.)

Data protected with AES encryption may not be sent out of the country due to export restrictions. This is not considered to be an issue as the Credit Union does not do business with trading partners outside of the United States.

Hashing algorithms (i.e. MD5 or SHA1) are not approved for protecting sensitive data stored on tape.

6.1 Data encryption protocols approved for sensitive data:
- AES – Advanced Encryption Standard, FIPS197 approved, using 128-bit and 256-bit key lengths. Symmetrical algorithm.
- 3DES – Triple Data Encryption Standard, FIPS approved, using 128-bit key length. Symmetrical algorithm.
- PGP – Pretty Good Privacy using public key infrastructure, with 1024-bit or greater key lengths. Asymmetrical algorithm.

7.0 Cryptoperiods

A cryptoperiod is the time span during which a specific key is authorized for use or the keys for a given system will remain in effect. A suitable period limits the use of a particular algorithm to its estimated lifetime, limits the time available for attempts to penetrate physical, procedural, and logical access mechanisms that protect the key from unauthorized disclosure. The cryptoperiod should be long enough that it does not create undue operational challenges but not so long that it creates weaknesses in protection.

7.1 Cryptoperiod for internally-used AES keys:
- 7.1.1 Data encrypted using AES with keys of 128 bits or longer for internal use should have a cryptoperiod of 12 months *with the following exceptions:*
  - 7.1.1.1 Permanently archived backup tapes (i.e. End-of-Month tapes) will use a *non-expiring* AES key
  - 7.1.1.2 Non-expiring AES keys may only be used for permanently archived backups stored in secure storage
  - 7.1.1.3 A given non-expiring AES key may protect a maximum of 24 months worth of permanently stored backups, after which a new non-expiring key must be used.

7.2 Cryptoperiods for third parties
- 7.2.1 AES Keys for third parties should use a cryptoperiod of 12 months unless the situation dictates a shorter cryptoperiod. The iSeries security officer is responsible for choosing an appropriate cryptoperiod for use with third parties based on the following variables:
- 7.2.2 Expected lifespan of encrypted data. If the lifespan is less than 12 months, a shorter cryptoperiod may be used
- 7.2.3 Ability of third party to properly secure the key materials. Shorter cryptoperiods should be established for third parties with less ability to properly secure key materials.

7.3 Non-auto expiring cryptoperiods
- 7.3.1 The Alliance AES encryption keys have no facility for automatically expiring key materials. Keys must be expired manually by the iSeries Security officer.
- 7.3.2 When key materials are expired, a notice to all operations staff must be made and posted to the Ops Intranet page that new keys are now in use. It is the responsibility of the Operations manager to notify staff of expired and new keys.

7.4 Cryptoperiods will be evaluated annually and adjustments may be made based on
- 7.4.1 Encryption technology advances
- 7.4.2 Discovered weaknesses in deployed algorithms
- 7.4.3 Operational efficiencies
- 7.4.4 Key handling efficiencies
- 7.4.5 Key storage concerns

8.0 Key Material Handling Protocols

There is no fail safe solution for encryption on any platform. The security of data is dependent on the appropriate management of encryption keys and passwords, the proper use of encryption commands and/or APIs, and the proper management of access to the computing platform and facility.

There is no way to recover encrypted data if the key is lost.

- 8.1 iSeries Alliance AES Key Handling Protocols
  - 8.1.1 The ANAESK and AEHIST files must be secured using iSeries object security per policy. *PUBLIC access must be removed.
  - 8.1.2 AETRI2 and AEACT2 (license file material) objects must not be mirrored to another system
  - 8.1.3 Encryption keys must not be backed up to the same media (i.e. tape) as data protected with that key
  - 8.1.4 Keys must be stored on the iSeries computer in order to be used
- 8.2 Generation of key materials
  - 8.2.1 Only authorized individuals (use chart below) may generate new keys
  - 8.2.2 Before new key materials are elevated to production they must be backed up to tape and relocated to approved off site storage
- 8.3 Online storage of key materials
  - 8.3.1 Only keys used for encrypting data to tape should be stored online on the iSeries
  - 8.3.2 Keys used for encrypting data on the file system should not be stored online on the same system
  - 8.3.3 Current keys will be stored on each iSeries system (PROD, HA, QC, DEV, I/P)
    - 8.3.3.1 Keys for franchise organizations, self processors, and third parties will be stored on the relevant iSeries computer until 90 days beyond the end of the cryptoperiod
    - 8.3.3.2 Keys must be on the iSeries computer in order to be used
- 8.4 Use of Split Keys
  - 8.4.1 The Credit Union does not currently use split keys. Backup and storage of split keys requires twice the overhead of non-split keys (i.e. the halves cannot be stored together) and the added security is not worth the overhead.
- 8.5 Escalation of key materials into the production environment
  - 8.5.1 Only authorized personnel may place new keys into production (see chart below)
  - 8.5.2 When new keys are placed into production, the Operations manager must be notified. It is the responsibility of the Operations manager to notify Operators that new keys are in production and that deprecated keys must no longer be used for new backups.
- 8.6 Copies of key materials
  - 8.6.1 Can be made to tape for disaster recovery purposes only
  - 8.6.2 Can only be made by authorized individuals
  - 8.6.3 Must NOT be stored with media containing data protected by those key materials
  - 8.6.4 Copies of keys must not be stored outside of the approved Alliance file library
- 8.7 Working with keys
  - 8.7.1 To prevent errors keys should not be manually entered to perform tasks. Keys should be accessed via custom programmatic controls
  - 8.7.2 Custom backup and restore menus have been created on the iSeries system. Keys are stored in modules and accessed via menu controls locked down by user profile according to the user rights chart included with this policy.
- 8.8 Offline storage of key materials
  - 8.8.1 Two copies of key materials should be stored in a locked fireproof safe in the vault room (aka “balance room”) of two board-approved client CUs. (i.e. Berrien Teachers and Western Districts). Two copies in each safe will allow one copy to remain to facilitate disaster recovery testing, while leaving one set remaining in the vault.

8.8.2 Written agreements with host client CUs detailing the storage agreement and guaranteed hours of access including after hours access procedures with contact numbers must be kept on file with Accounting and included in applicable disaster recovery documentation.
8.8.3 Only authorized individuals will have access to the vault storage
8.8.4 One copy will be stored in a locked fireproof safe in the archives room at the 28th Street location ("onsite").
8.8.5 An up to date table with issued key names (see 9.1.1.3) shall be stored with each copy of the key materials

8.9 Electronic transportation of key materials
8.9.1 Key materials may be transmitted electronically between systems on the Credit Union's private network by authorized personnel
8.9.2 Key materials may only be transmitted electronically outside the Credit Union's private network when encrypted by an approved encryption algorithm. Transportation may only be made by authorized personnel.
8.9.3 A log detailing the transportation (movement) of keys including key names, who transported the keys, and dates of the transport must be kept in the vault with the backup copies of the keys. All key movement must be logged.

8.10 Physical Transportation of key materials
8.10.1 Keys may only be transferred by authorized individuals of the Credit Union
8.10.2 A log detailing the transportation (movement) of keys including key names, who transported the keys, and dates of the transport must be kept in the vault with the backup copies of the keys. All key movement must be logged.

8.11 Lost or compromised key materials
8.11.1 Suspected lost or compromised key materials should be immediately reported to the security team via a security incident report. The team should use normal procedures for investigating and reporting the possible breach to senior management and the board of directors.
8.11.2 If a key has been determined to have been lost or compromised the following should take place as soon as practical:
- Use of the compromised key should be suspended immediately
- A new key should be generated
- Data protected with the compromised key must be either re-encrypted with the new key or destroyed
- Compromised keys should be deleted once materials encrypted with the compromised keys have been re-encrypted with newly issued keys
- All actions must be documented and attached to the relevant security incident report

8.12 Use and Handling of Expired Keys
8.12.1 Expired keys should remain on the system for 90 days after the key expiration date to facilitate restores.
8.12.1.1 Copies of expired keys should remain in secure storage for the duration of the lifespan of data protected with the key unless that data is re-encrypted with current key
8.12.1.2 Expired keys should be removed to secure storage after 90 days
8.12.1.3 Expired keys must not be used to encrypt new data.

8.13 Personnel Authorized to Work with Key Materials

8.13.1 Access to key functions should be strictly controlled to maintain key and protected data integrity. Use of key backup privileges should be severely restricted to prevent unauthorized copies of keys.

8.13.1.1 Users who can create keys should not be allowed to transport keys

8.13.2 Authorized personnel and allowed actions are detailed below. Roles of authorized personnel are outlined in the Data Security Policy

User/Department	Backup	Restore	Create Keys	Place Keys into Production	Backup Keys	Expire Keys	Delete Expired Keys	Physical Transport Keys/Vault Access	Electronic Transport of Keys
Operations	Y	Y	N	N	N	N	N	N	N
iSeries Security Officer	Y	Y	Y	Y	Y	Y	Y	N	N
iSeries Administrator	Y	Y	Y	N	Y	N	N	N	N
CEO	N	N	N	N	N	N	N	Y	N
CFO	N	N	N	N	N	N	N	Y	N

9.0 iSeries System (Tape) Encryption Protocols

The iSeries computer uses software encryption to encrypt member data stored on backup tapes using 128-bit or 256-bit AES algorithms.

9.1 Key Naming Convention

9.1.1 One key will be used per organization to simplify key management and allow encryption/decryption tasks on any machine. The key will need to be installed on all machines

9.1.1.1 Use of different keys for each system is considered unnecessary

- Creates a source of confusion for operators. Operators may choose the incorrect key, creating confusion during restoration
- All keys would need to be on all systems anyway to facilitate restoring tapes encrypted on one machine and restored on another
- Key material handling and storage protocols are the same. As keys will be stored in the same location, use of separate keys does not increase security
- Backup tapes are stored in same locations. Use of separate keys does not increase security

9.1.1.2 Key names use a 10 byte field and shall be named as follows:

Organization ID	Key Creation Date	Cryptoperiod in Months
2 Bytes Alphanumeric ____ ____	6 Bytes Numeric *YYMMDD*	2 Bytes Numeric

9.1.1.3 A list of all key names issued will be kept up to date by Operations management. A copy of the table and list will be kept offsite

9.1.1.4 Keys may ONLY be used internally. They may NOT be shared with third parties or vendors

9.1.1.5 Keys will comply with established cryptoperiods

9.1.1.6 Examples:

9.1.1.6.1 A key issued for internal use to encrypt backups on 3/1/2006 with a cryptoperiod of 12 months would be named: CU06030112

9.1.1.6.2 A key issued for encrypting data sent to a statement processor on 5/15/2006 with a cryptoperiod of 6 months would be named: SD06051506

9.2 Backup tape labeling

9.2.1 Backup tapes will be labeled with the key name used to encrypt the tape.

9.3 Pass phrases

9.3.1 Pass phrases are an “on-the-fly” method of encrypting data instead of using previously defined keys. Because of the necessity in maintaining control over the encryption process, use of pass phrases to encrypt to tape is not permitted.

10.0 Audit Procedures

10.1 To ensure these procedures are being followed audits of this policy should be conducted by the accounting department every quarter.

10.2 Audit results for the most recent quarterly audit must be reported to the board of directors at the next board report interval.

10.3 Serious deficiencies discovered during an audit must be immediately reported to the security team for follow-up action.

10.3.1 As soon as practicable, the security team must file a full report of the deficiency and corrective actions taken to senior management and the board of directors.