ANEJO C

BUSINESS CONTINUITY PLAN

VERSION 2009

Mainframe Disaster Recovery Plan

BUSINESS CONTINUITY OFFICE

Guide for Mainframe Disaster Recovery Plan

Table of Contents

Introduction

The Business Continuity Plan for Mainframe establishes the procedures to follow when recovering the UI Mainframe operations following a disruption. This Mainframe Recovery Plan applies to the functions, operations, and resources necessary to restore and resume EVERTEC's Mainframe operations at its primary location (Cupey Campus, San Juan) and alternate site's (Tres Monjitas and Sungard).

Internal and external threats such as Malicious Activity, Natural Disaster and Technical Disaster, may initiate the activation of the Mainframe Recovery Plan:

A. Malicious Activity.
   1. Fraud, Theft, or Blackmail
   2. Terrorism

B. Natural Disaster
   1. Fire
   2. Floods and other water damage
   3. Severe weather (earthquake, hurricane, or tornado)
   4. Air contaminants
   5. Hazardous chemical spill

C. Technical Disaster
   1. Communications Failure
   2. Power Failure
   3. Equipment and Software Failure
   4. Transportation System Disruption

If any of the above threats occur and/or the following criteria are met:

1. Mainframe is unavailable or damaged.
2. Facility is damaged and will be unavailable.

Either the Business Continuity Coordinator or/and the Mainframe Recovery Team Leader will be notified of the emergency situation. Either of them will notify the EMT (Emergency Management Team) and the EMT will declare the emergency and activate the Mainframe Recovery Plan.

The Mainframe Recovery Team Leader will brief his team of the emergency, prepare a work schedule and determine if relocation is required.

The Mainframe Recovery Team tasks are defined in this document and the roles and responsibilities are defined in the Standards and Guidelines manual.

The Business Continuity Coordinator will notify the alternate site at Tres Monjitas or the tertiary location at Sungard that a disaster has been declared and to prepare the facility for EVERTEC's arrival.

The mainframe computer is large and more powerful than other platforms, it does not have the inherent redundancy that a distributed system or network provides. As a result, mainframe availability and data backups are critical. The following measures were considered when determining mainframe contingency requirements:

1. **Store Backup Media Offsite.** Backup media was labeled, logged, and stored offsite in a secure, environmentally controlled facility. The storage facility is located far enough away from Cupey Campus to reduce the likelihood that both sites would be affected by the same event.

2. **Document System Configurations.** Detailed records of system configurations, hardware, software, communications and other vital documentation have been prepared and backed-up.

3. **Personnel Availability.** Key personnel have been identified and contingencies are in place should those employees not be available. Accommodations and services to employees' family members will be provided if necessary. Please refer to the Standards and Guidelines manual.

4. **Vendors.** A service level agreement is in effect with all vendors that supply essential hardware, software, and other components.

5. **Security Policy and System Security Controls.** Mainframe contingency security will be coordinated through the Network Security Policies and Data Security Department.

6. **Hardware and Software Inventory.** A list all the mainframe hardware and software needed to continue operations is located at the Off-Site Storage Site.

1 Stage 1: Response

1.1 Immediate Response

1.1.1 Receive Information about a Business Disruption

When receiving information about a disruption to your Business Unit, use the "Initial Contact Report" (Appendix A) form to document the details of the disruption. If the call received comes from an entity outside the Corporation, notify this fact and disruption details immediately to your Supervisor or Business Continuity Coordinator (BCC).

1.1.1.1 Business Continuity Coordinator Information

- See Appendix B for Business Continuity Coordinators information.

1.1.2 Alert the Recovery Team Members

Inform the details of the disruption to the Mainframe Recovery Team and request that they be ready to receive instructions. Perform the necessary tasks to contact them.

1.1.2.1 Team Members Information

- See Appendix C for Recovery Team Members information.
- Evaluate Facilities and IBM Mainframe Conditions

The Mainframe Recovery Team Leader will coordinate the damage evaluation process with Computer Centers Administration to evaluate disruption impact on operational conditions and facilities, including access to affected areas. If

possible, take pictures of equipment and facilities in damaged areas for insurance claim purposes. Determine if equipment and facilities are usable.

1.1.2.2 Contact Information List for Computer Center Administration

- See Appendix D for Computer Center Administration information.

1.1.3 Contact Support Staff

The Recovery Team will call staff members of all related Mainframe Support units, including Systems Engineering, Network Engineering, Information Security, Storage Systems, Computer Operations, Programming, and Computer Centers Administration to provide recovery status information. Make sure that all staff members know your telephone number(s) and how to get recovery status announcements.

- Please refer to the Communications and Human Resources section in the Standards and Guidelines manual.
- See Appendix E for Staff Information.

1.1.4 Receive Instructions about Mainframe Recovery Plan Activation

The EMT will evaluate the disruption situation, declare an emergency, and activate the Mainframe Recovery Plan.

- Please refer to the Standards and Guidelines manual (EMT at-time-of –disaster responsibilities section)
- See Appendix F for Emergency Management Team information.

1.1.5 Activate the Recovery Team Members

Inform the Mainframe Recovery Team that an emergency has been declared and the recovery plan is activated. The Mainframe Recovery Team Leader will assign responsibilities and prepare a work schedule.

1.1.6 Determine Which Recovery Strategy to Implement

The Mainframe environment is composed of two tiers for recovery purposes.

A local recovery of the Mainframe can be performed at the Business Recovery Center at Tres Monjitas. A remote recovery of the Mainframe can be performed at Sungard's Recovery Center at Philadelphia, PA.

There are two scenarios, each with a specific implementation strategy, based on the following:

Scenario	Strategy to implement
1. Cupey Campus processing facility is unavailable / inaccessible and Tres Monjitas is operational.	Relocate Mainframe operations to the Business Recovery Center at Tres Monjitas.
2. Cupey Campus processing facility and Tres Monjitas are unavailable / inaccessible.	Relocate Mainframe operations to Sungard's Recovery Center at Philadelphia. Refer to Standard's and Guidelines Manual, Travel Coordination section.

1.1.7 Start Relocation process to the selected Recovery Site

The Business Continuity Coordinator will call and inform the selected site a disaster has been declared and a relocation strategy is in place.

- Use the instructions in Appendix G to declare a disaster and start relocation at the Business Recovery Center at Tres Monjitas.
- Use the instructions in Appendix H to declare a disaster and relocate at Sungard's Recovery Center at Philadelphia, PA.

1.1.8 Notify Key Vendors That Will Support Recovery Operations

Notify the Key Vendors or Suppliers that will support your recovery efforts. Before contacting vendors, determine the following:

1. The specific information about the business interruption that is appropriate for communicating to the vendor.

2. The specific action, support, services, and other resources required from the vendors to implement and sustain your functional recovery response.
3. Your expectations with regard to the timing or need for actions, support, services, and other resources.
4. The name of the assigned employee(s) or alternate employee(s) that will contact each vendor.

1.1.8.1 List of Vendors by Departments

- See Appendix I for List of Vendors information.

1.1.9 Notify Key Contacts that will support Recovery Operations

Notify the key internal and external contacts that will support your recovery. Before notifying your key contacts, determine the following:

1. The specific information about the business interruption that is appropriate to communicate to each contact.
2. Specific action, support, services, and other resources you may require.
3. Your expectations regarding the timing.
4. The name of the assigned employee(s) or the alternate(s) that will contact each key contact.
   - See Appendix E for Staff Information.
   - See Appendix J for Other Contact Information.

1.1.10 Record Recovery Expenses

Keep a record of all recovery expenses with supporting documents. This information is important for quantifying recovery costs and handling insurance claims. Please refer to the Recovery Support and Control section in the Standards and Guidelines manual.

1.1.11 Report Response Status to EMT/BCC

The Mainframe Recovery Team will provide an update of the Response process to the EMT/BCC.

2 Stage 2: Relocate

2.1 Confirm Alternate Site Requirements

According to the scenario chosen in the *Recovery Strategy Section*, select the appropriate relocation site:

- Tres Monjitas - section 2.1.1 Confirm your Relocation to Tres Monjitas
- Sungard - section 2.1.2 Confirm your Relocation to Sungard.

2.1.1 Confirm your Relocation to Tres Monjitas

Confirm with Computer Center Administration if Tres Monjitas is available and receive authorization from the EMT to initiate the relocation process.

See Appendix D for Computer Center Administration.

See Appendix G for disaster notification procedures at Tres Monjitas.

2.1.1.1 Validate the Resource Requirements to Recover in Tres Monjitas

Gather the Mainframe Recovery Team to:

1. Validate the specific equipment and quantities required to resume your functions at Tres Monjitas.
2. Coordinate with the various support teams to obtain the necessary resources.
3. If necessary, fill in the Gen-230 (Equipment Requisition) and send it to the Command Center.

Equipment Inventory in Puerto Rico

See Appendix X for Equipment Inventory information.

Off-Site Magnetic Media Back-Up Inventory

- See Appendix Y Off Site Magnetic Media Control for Backup Inventory information.

2.1.1.2 Determine Transportation Requirements for Tres Monjitas

The Mainframe Recovery Team Leader will appoint a person to act as a single point of contact for the Team.

Coordinate the following with Computer Centers Administration:

1. The scheduling of couriers and the movement of salvaged inventory.
2. Movement of inventory to Tres Monjitas.
3. Ensure that all customers that exchange physical data (tapes, reports, etc…) are informed of the relocation to Tres Monjitas.
   - See Appendix B for Business Continuity Coordinators information
   - See Appendix FF for Directions to Tres Monjitas

2.1.1.3 Verify the availability of Off-Site Storage Box at Tres Monjitas

Make sure all indispensable materials for Mainframe Recovery are available at you the off-site storage box at Tres Monjitas.

- See Appendix K for the Off Site Storage Box Inventory information.

2.1.1.4 Confirm availability of Mainframe backups at Tres Monjitas

Confirm with Computer Operations Group the availability and setup of backup tapes at Tres Monjitas.

- See Appendix L for Librarian Contact List information.

2.1.1.5 Notify of New Work Location

The Command Center will notify key contacts of your new work location (Tres Monjitas).

↳ See Appendix E for Staff Information.

2.1.1.6 Verify resource requirements at Tres Monjitas

The Mainframe Recovery Team Leader will verify that the requisition was received and processed at the Command Center. After receiving the equipment, the Mainframe Recovery Team Leader verifies it has been installed and all necessary communications are activated. If experiencing functionality problems contact the Command Center again.

2.1.1.7 Support Salvage Operations

The Mainframe Recovery Team Leader will select a representative(s) to work with the Facilities Restoration and Relocation team in the salvage operations.

1. Verify the conditions of the Salvage Inventory at Cupey Campus.
2. Transport Salvage Inventory to Tres Monjitas as soon as you have access to the site.
3. Use the Salvage Inventory List to verify that all items are salvaged (CD copies in Tres Monjitas and Cupey and hard copies in Tres Monjitas, Cupey and PC).
4. Use the Floor Map to identify the location of the Salvage Inventory.

↳ See Appendix W for Cupey Campus Floor Map information.

- See Appendix AA for Salvage Inventory information.

2.1.1.8 Analyze How to Re-Initiate the Daily Production Run

The Programming and Operations Departments will determine the strategy to follow to initiate the recovery of the daily production run at Tres Monjitas based on point of failure that the Storage System identified.

- See Appendix Z for Daily Production Run Procedures information
- See Appendix E for Staff Information

2.1.2 Confirm your Relocation to Sungard

Validate with Sungard if the site is available and receive authorization from the EMT to relocate.

- See Appendix H for Sungard Contact information.

2.1.2.1 Validate the Resource Requirements to Recover at Sungard

The Business Continuity Coordinator will contact Sungard to determine if the specific equipment, quantities required, and indispensable materials for Mainframe recovery are available to resume our functions at Sungard.

Equipment Inventory

See Appendix DD for Equipment Inventory at Sungard information.

2.1.2.2 Determine Transportation Requirements

The Mainframe Recovery Team will contact the Recovery Administration Team at the Command Center to make travel arrangements for the personnel in charge of Mainframe Recovery at Sungard.

- Please refer to the Recovery Administration section of the Standards and Guidelines manual for travel arrangements information
- See Appendix B for the Business Continuity Coordinators contact information.
- See Appendix II for Directions to Sungard Information.

2.1.2.3 Confirm availability of Mainframe Backups

Confirm with Computer Operations the availability and setup of backup tapes to transport to Sungard.

- See Appendix L for Librarian Contact List information

2.1.2.4 Notify of New Work Location

Mainframe Recovery Team will notify the Command Center of relocation to Sungard.

2.1.2.5 Analyze how to re-initiate the daily production run

The Programming and Operations Departments will determine the strategy to follow to initiate the recovery of the daily production run at Sungard.

2.2 Report Relocate Status to EMT/BBC

The Mainframe Recovery Team will provide an update of the Relocation process to the EMT/BCC.

3 Stage 3: Recover

3.1 Restore the IBM Mainframe

The Mainframe Recovery Team Leader will assign the following tasks to the corresponding team member.

- Refer to Appendix C for Mainframe Recovery Team members' information.

3.1.1 Restore the IBM Mainframe Operating System

- See Appendix M for instruction on the restoration for Cupey's LPAR.
- See Appendix N for instruction on the restoration for Río Piedras' LPAR.

3.1.2 Configure Security Parameters

- See Appendix O for configuration of security parameters for Cupey's LPAR.
- See Appendix P for configuration of security parameters for Río Piedras' LPAR.

3.1.3 Configure ATL/VTS – Tres Monjitas

- See Appendix Q for Activation Procedure for the 3494 library and VTS at Tres Monjitas for Cupey's LPAR.
- See Appendix R for Activation Procedure for the 3494 library and VTS at Tres Monjitas for Rio Piedras' LPAR.

3.1.4 Configure ATL/VTS - Sungard

- See Appendix S for Activation Procedure for the 3494 library and VTS at Sungard for Cupey's LPAR.

3.1.5 Restore the IBM Mainframe Network Connectivity

- See Appendix T for the Network Connectivity Procedure.

3.1.6 Configure the IBM Mainframe Connectivity and Online Facilities

- See Appendix M for Operating System, Connectivity, and Online Facilities Restoration information.

3.1.7 Restore the IBM Mainframe Applications

- See Appendix V for Applications Restoration Procedures information.

3.1.8 Restore Mainframe Communications

- See Appendix BB for Mainframe Communications Recovery information.

3.1.9 Report Recovery Status to EMT/BCC

The Mainframe Recovery Team will provide an update of the Recovery process to the EMT/BCC.

4 Stage 4: Restore

4.1 Resume Business Functions

4.1.1 Evaluate Operational Status

After the critical processes have been recovered, determine the necessity to continue the recovery of non-critical processes according to the interruption scenario. Use the different support teams to coordinate the requirements that will be necessary for the recovery of these non-critical processes.

Critical applications will be given priority as well as those applications that give support to the critical applications.

4.1.2 Resume Daily Run Operations

Start the daily batch process and notify application owners/users when the operations can be resumed. Make sure that the daily backup tapes are being generated and rotated off-site.

4.1.3 Provide Support for Facility Restoration

The Facilities, Restoration, and Relocation Team is responsible for coordinating the structure restoration process and will contact the Mainframe Recovery Team when assistance is required. Please refer to the Facilities, Restoration, and Relocation section of the Standards and Guidelines Manual for the responsibilities of the team.

4.1.4 Report Restore Status to EMT/BCC

The Mainframe Recovery Team will provide an update of the Restore process to the EMT/BCC.

5 Stage 5: Return

5.1 Relocate from the Selected Alternate Site to an Interim Facility

5.1.1 Support the Move to Interim Facilities

The Facilities, Restoration, and Relocation Team will be coordinating the movement to the interim facility after receiving the instructions from the Command Center.

5.1.2 Notify your Contacts about the Move

The Command Center will notify key contacts of your new work location at the Interim Facility.

5.2 Return Operations to the Permanent Site

5.2.1 Coordinate With the Facilities, Restoration, and Relocation Team and Computer Centers Administration to Plan the Move to the Permanent Site

- Make sure all necessary resources and equipment are available at the permanent site.
- Coordinate the move of the off-site backup tapes to the permanent site.
- Plan the cut off time for the daily batch process.

5.2.2 Coordinate a Move Date

Schedule the move on a weekend if possible to minimize disruption of processing and customer interface.

5.2.3 Notify your Contacts about the Move

The Command Center will notify key contacts of your new work location at the permanent site.

5.2.4 Restore and Resume Operations on Permanent Site

5.2.4.1 Restore the IBM Mainframe Operating System

- See Appendix M for instruction on the restoration for Cupey's LPAR.
- See Appendix N for instruction on the restoration for Río Piedras' LPAR.

5.2.4.2 Configure Security Parameters

- See Appendix O for configuration of security parameters for Cupey's LPAR.
- See Appendix P for configuration of security parameters for Río Piedras' LPAR.

5.2.4.3 Restore the IBM Mainframe Network Connectivity

- See Appendix T for the Network Connectivity Procedure.

5.2.4.4 Configure the IBM Mainframe Connectivity and Online Facilities

- See Appendix M for Operating System, Connectivity, and Online Facilities Restoration information.

5.2.4.5 Restore the IBM Mainframe Applications

- See Appendix V for Applications Restoration Procedures information.

5.2.4.6 Resume Daily Run Operations

Start the daily batch process and notify application owners/users that regular operations have been resumed. Make sure that the daily backup tapes are being generated and rotated to the off-site.

5.2.5 Report Return Status to EMT/BCC

The Mainframe Recovery Team will provide an update of the Return to Operations process to the EMT/BCC.

Appendixes – Table of Contents

ANEJO D

GOBIERNO DE PUERTO RICO
DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS
OFICINA DE CÓMPUTOS Y SISTEMAS

4 de febrero de 2010

Sra. Alba Maldonado Colon
Directora, Oficina Auditoría Interna

CERTIFICACIÓN AUDITORIA

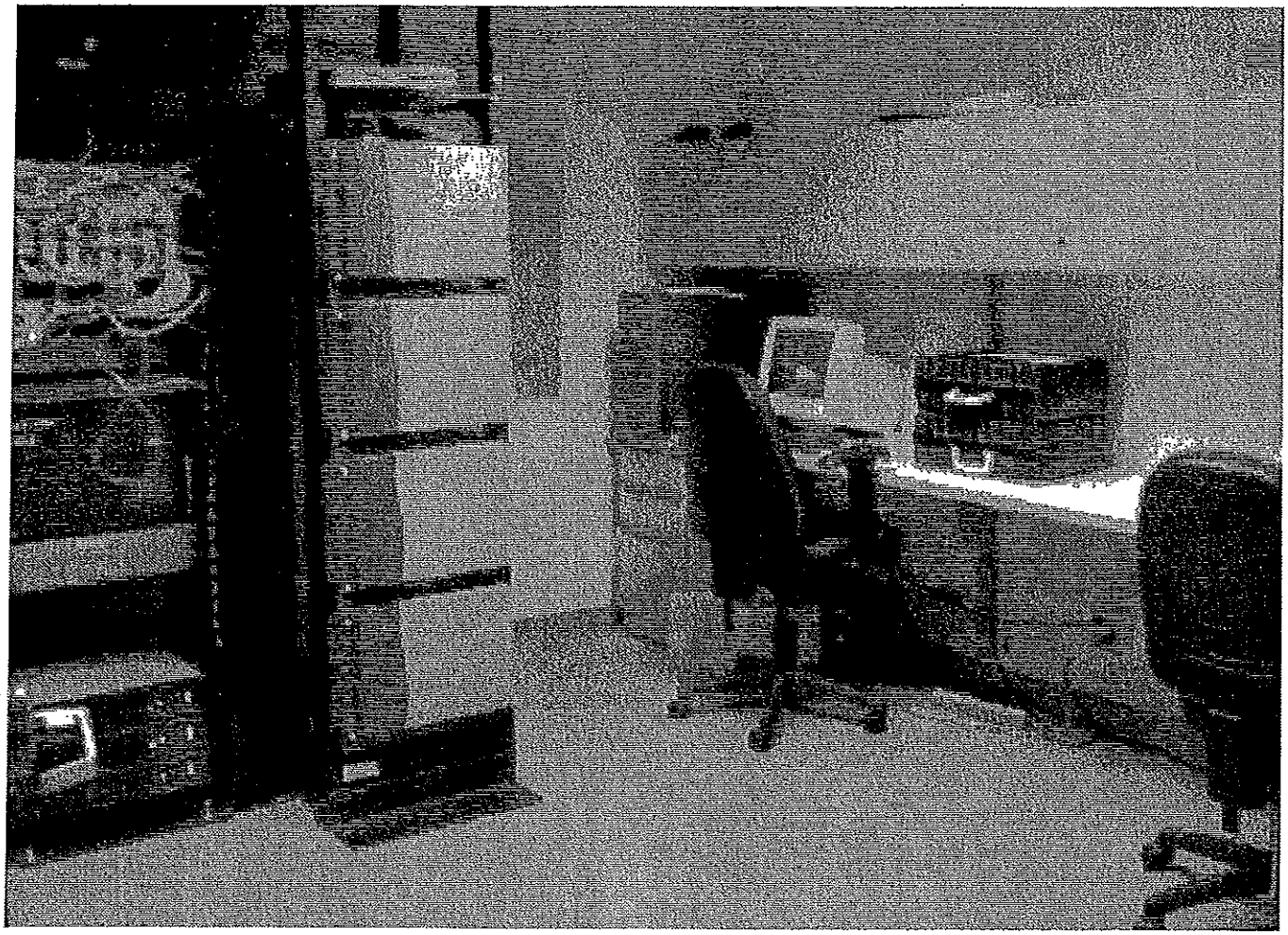
Saludos. Por la presente le confirmo que en cumplimiento con la recomendación realizada en la auditoria TI-0914 tenemos ubicado un volumen de la Descripción y configuración de operación y recuperación de los servidores centrales y locales del DTRH.

Se le incluye foto del punto de disposición ubicado en el 2do piso del edificio del NSE, en el nodo de comunicaciones de la Oficina de Cómputos y Sistemas.

Para cualquier duda o información adicional favor de comunicarse con este servidor.

José A. Ríos

Sr. José A. Ríos
Director
Oficina de Cómputos y Sistemas



Facilidades negociado Seguridad de Empleo utilizadas por la Oficina de Cómputos y sistemas.

ALBA MALDONADO COLON

From: AUREA RIVERA NEGRON
Sent: Friday, September 25, 2009 8:21 AM
To: ALBA MALDONADO COLON
Subject: ICP-1- INFORME DE AUDITORIA TI-09-14

Saludos , Buenos Días:

En cuanto al Borrrador entregado por la Oficina de Personal le especifíco lo siquiente,

Rec. 6.b- Deberán someter evidencia del Plan de Clasificación y Retribución e Identificar los Puestos del Personal de la OCSI.
o sí esta el proceso de elaborar nuevo Plan , entonces seria Parcialmente cumplimentada.

Rec. 6.d- Deberán someter evidencia como Hoja de Trámite , o Certificación de que el Proceso se llevó a cabo, de lo contrario
se deberá identificar como Parcialmente Cumplimentada.

WAGP02PL DEPARTAMENTO DEL TRABAJO FECHA: 09-02-0
DECLARACION TRIMESTRAL DE SALARIOS USUARIO: $7D2
PAGADOS A CADA EMPLEADO
MANTENIMIENTO DE SALARIOS

BATCH: 2954 TRIMESTRE: 092 FORMA AAT PATRONO: 335210000

ELI	SEGURO SOCIAL	CLAVE ALPHA	SALARIO
	581 11 8235	NEGR	0317000
	582 29 9102	MAYM	0233180
	582 41 1358	SANT	0300636
	582 41 1551	RIVE	0296800
	582 43 4254	CATA	0077000
	583 07 6477	ROSA	0225320
	583 27 2695	COLL	0538470
	583 33 5597	COLO	0235800
	583 49 8054	MARR	0368414
	583 54 4218	OTER	0382520
	583 61 6035	FONT	0309160
	583 63 0189	SANT	0392992
	583 67 6005	FEBU	0520000

PF1=SALIR PF2=PROXIMA PANTALLA PF3=MENU PRINC. PF5=ACTUALIZAR ENTER=VALIDAR
ENTRE DATOS A MODIFICAR O PRESIONE PF5 PARA ACTUALIZAR WAG0

ANEJO E

Estado Libre Asociado de Puerto Rico
Departamento del Trabajo y Recursos Humanos
Oficina de Cómputos y Sistemas

Hoja de Solicitud de Accesos a Sistemas

Información de Usuario:

Apellidos: _____ Puesto: _____
Nombre: _____ División: _____
Inicial: _____ Oficina: _____
Teléfono: _____ Piso: _____

¿Empleado DTRH? ☐ SI ☐ NO - Nombre de la Compañía _____

Fecha de la Solicitud: _____

Acción Requerida:

☐ Usuario Nuevo ☐ Modificar Usuario ☐ Eliminar Usuario

Tipo de Acceso:

☐ Acceso a la Red (LAN)
- ☐ Outlook
- ☐ Internet
- ☐ Prifas

☐ Acceso a Interempleo
- ☐ # Station/desk asignado: _____
- ☐ NAL ☐ MUNIS

☐ Acceso a Saben
- ☐ DL
- ☐ Contribuciones

☐ Cuadro Teléfonico
- ☐ Extención _____

Nivel de Acceso
- ☐ Área Metro
- ☐ Área Metro / Isla
- ☐ Área Metro / Isla / EEUU
- ☐ Área Metro / Isla / EEUU / Internacional

Justificación:

_____
_____
_____

Entiendo y estoy de acuerdo que las cuentas de acceso son confidenciales e intransferibles, en utilizarlas para las tareas asignadas y con las normas establecidas según la Política General de Administración de Sistemas de Información vigente.

Firma del Empleado: _____ Fecha: _____

Aprobado por:

Nombre del Supervisor: _____ Fecha: _____

Firma: _____

Para uso de Administración: NO ESCRIBA NADA AQUÍ

Red	Saben	Interempleo	Otros	Cuadro Teléfonico
Username: _____	UserId: _____	User: _____	Munis: _____	Código: _____
Password: _____	Password: _____	Password: _____	Nal: _____	

Email: _____

Solicitud ☐ Aprobada ☐ Denegada

Comentario: _____

APROBADA POR: _____ Fecha: _____

PROCESADO POR: _____ Fecha: _____

Rev. 4/23/2009

ANEJO F

Department of Labor & Human Resources (DOL)

Security Infrastructure Project

Network Discovery Documentation

Pre-Implementation

September 1, 2009

Introduction

The EVERTEC security team focused in the implementation of a new security network infrastructure takes the initiative to realize, as a first step, a network discovery. The intention of this network discovery is to capture and inform the actual network infrastructure (IT Assets) of DOL and its different status.

This document will introduce a security implementation recommendation based on the best security practices. All recommendations that are in place could be ignored.

Data Collected

Main Building

Six Floor Network Discovery

Switches

LAN

Seven and Eight Floor Network Discovery

Switches

LAN

Nine, Ten and Eleven Floors Network Discovery

Switches

LAN

Twelve Floor Network Discovery

Switches

LAN

Fourteen Floor Network Discovery

Switches

LAN

Fifthteen, Sixteen and Seventeen Floors Network Discovery

Switches

LAN

Eighteen Floor Network Discovery

LAN

Twenty One Floor Building Network Discovery

Switches

LAN

Main Core Switches

Main Switches

Main Routers

Router

Router to ADT

Router to EVERTEC

WAN Communication Cloud

Coamo Regional Office
- **WAN**
- **LAN**

Fajardo Regional Office
- **WAN**
- **LAN**

Manati Regional Office
- **WAN**
- **LAN**

Caguas Regional Office

WAN
LAN

Guayama Regional Office

WAN
LAN

San German Regional Office

WAN
LAN

Vieques Regional Office

WAN
LAN

Humacao Regional Office

WAN
LAN

Arecibo Regional Office

WAN
LAN

Carolina Regional Office

WAN

LAN

Mayaguez Regional Office

WAN

LAN

Aguadilla Regional Office

WAN

LAN

Ponce Regional Office

WAN

LAN

Bayamon Regional Office

WAN

LAN

Real Hermanos Regional Office

WAN

LAN

Anejo DOL Central

WAN
LAN (172.16.104.1)
LAN (192.168.104.1)

EBT to DOL 3M

WAN
LAN

EBT to DOL CU

WAN
LAN

Recommendations

These recommendations are based in the best security practices and network segregations.

Implementation of Network Security Segregation:

The EVERTEC security team suggests DOL to implement network security segregation between the IT Assets (servers) and the clients (workstations). The easiest and safest way to implement this consideration is creating three new network segments and maintaining the actual Data Center networks. The Data

Center Networks that will be maintained for the servers are, 172.16.6.0/24 and 146.146.0.0/16, and will be protected in a security zone (DMZ) behind the new Cisco Adaptive Security Appliance infrastructure. The three new separate networks will be as followed; the first one will be for the servers, workstations and network administrators; the second one for the programmers; and the third one for data entries. This type of network segmentation permits access controls granularity such as programmers having access only to the applications and development environments without obtaining directly access to the Microsoft Domains Controllers or to the Exchange Mail Console. And more important controlling and preventing the data entries and all DOL networks in the whole island to connect indiscriminately to the IT technology assets.

Implementation of Full Content and Control of Network Traffic:

The EVERTEC security team suggests DOL to implement the acquisition of the Cisco Content and Control Security Services Module (CSC-SSM). This security module will permit DOL Security Administrator to upscale their security controls and data content verification before entrance to the DOL networks and also before sent it to DOL customers, partners or government peers.

This upscale should be implemented using eight security technologies included in the new security infrastructure; Antivirus Perimeter Gateway, Anti-Spyware Security Gateway, Anti-Spam Security Gateway, Anti-Phishing Protection, Real-Time Protection for Web Access, Mail and File Transfers Controls, URL Filtering Capability and E-Mail Content.

Antivirus

Antivirus gateway technology shields internal network resources from virus attacks at the most effective point in your infrastructure, the Internet gateway. Cleaning e-mail and Internet web traffic at the perimeter helps ensures business continuity and eliminates the need for resource intensive malware infection clean-ups.

Anti-Spyware

Blocks spyware from entering the network through Internet web and e-mail traffic. Frees up IT support resources from costly spyware removal procedures and improves employee productivity by blocking spyware at the gateway.

Anti-Spam

Effectively blocks spam with extremely low false positives, helping to maintain the effectiveness of e-mail communications, so contact with customers, vendors, and partners continues uninterrupted and without distraction.

Anti-Phishing

Protection against spoofed identity and sourcing guards against phishing attacks thereby preventing employees from inadvertently disclosing company or personal details.

Real-Time

Even if company e-mail is already protected, many

Protection for Web Access, Mail and File Transfers	employees will access their own private Webmail from company PCs or laptops introducing another entry point for Internet-borne threats. Employees may also directly download programs or files that may be contaminated. Real-time protection of all Web traffic at the Internet gateway greatly reduces this often-overlooked point of vulnerability.
Full URL Filtering Capability	URL filtering can be used to control employee Internet usage by blocking access to inappropriate or non-work-related websites, thereby improving employee productivity and limiting the risk of legal action being taken by employees exposed to offensive Web content.
E-Mail Content Filtering	E-mail filtering minimizes legal liability due to exposure to offensive material transferred by e-mail and enforces regulatory compliance, helping organizations meet the requirements of legislation such as Graham Leach Bliley and the Data Protection Act.

Implementation of Administrator and Root Account Password Vault:

The EVERTEC security team suggests DOL to implement a password vault with high end encryption for the management of administrator, root and application administration accounts (known as Service Accounts). DOL should define a

request procedure with prior employee's management approval for access to the password vault. The access should be defined by the roles of DOL administration profiles such as UNIX administrators, Microsoft Domain Admins, Application Admins, etc. This request should be monitored for privilege changes and justifications of it.

Account password before vault usage should be address by immediately changed and vaulted.

Implementation of Administrator and Root Account Usage and Change Monitoring:

The EVERTEC security team suggests DOL to implement the monitoring of usage and changes made by the administrator, root or service accounts. DOL should implement security software that capture and classify the events in order by security criticality. This type of software will deliver notification of non authorized changes by the administrators and will consolidate the evidence of action and correlation of events in a centralized console.

Implementation of a Patch Management Procedure:

The EVERTEC security team suggests DOL to implement a Patch Management Procedure assurance the control of emergency patch notification and implementation; and the continuity of a healthy patch program. This procedure will prevent DOL for exploit of malicious codes and worms knowing by the operating system manufactures.

For this procedure to be accurate DOL Administrators should be registered to operating system (OS) and application security advisories notifications. All security notification should be evaluated by the OS administrator; if is consider or classified as critical or high impact, it should be implemented in fast track procedures; the mediums and low can be integrated the basic patch management procedure. It is important to maintained track of patch implementation.

Implementation of IT Assets Health Monitoring:

The EVERTEC security team suggests DOL to implement few protocols such as SNMP with a non known community string. This community string should not be the same one betweens the networking devices, servers and printers or Photocopies. The network administrator should implement a centralized management console for statistics and reports. This repots should be compare in a monthly basis for capacity planning.

Other important consideration should be the maintenance of the Microsoft Active Directory Replication, Domain Controller Priority Scheme and DNS health.