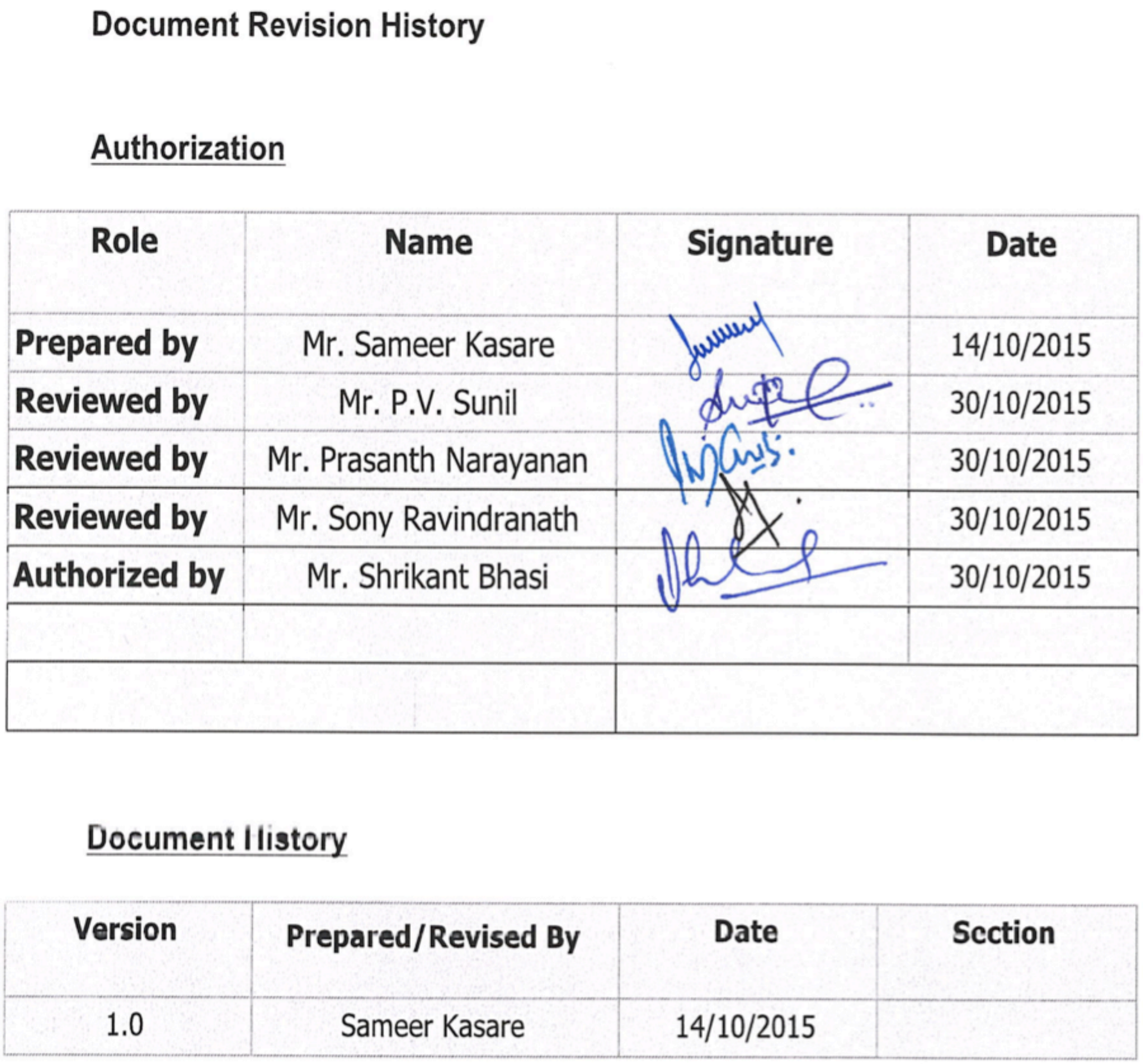
# CARNIVAL GROUP



## Document Revision History

### Authorization

| Role | Name | Signature | Date |
|---|---|---|---|
| Prepared by | Mr. Sameer Kasare | | 14/10/2015 |
| Reviewed by | Mr. P.V. Sunil | | 30/10/2015 |
| Reviewed by | Mr. Prasanth Narayanan | | 30/10/2015 |
| Reviewed by | Mr. Sony Ravindranath | | 30/10/2015 |
| Authorized by | Mr. Shrikant Bhasi | | 30/10/2015 |
| | | | |
| | | | |

### Document Ilistory

| Version | Prepared/Revised By | Date | Scction |
|---|---|---|---|
| 1.0 | Sameer Kasare | 14/10/2015 | |

## 1.0 Overview

1. The intentions for publishing an IT Policy are not to impose restrictions that are contrary to CARNIVAL GROUP Established culture of openness, trust and integrity. IT team is committed to protecting CARNIVAL GROUP Employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.
2. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of CARNIVAL GROUP. These systems are to be used for business purposes in serving the interests of the company.
3. Effective security is a team effort involving the participation and support of every CARNIVAL GROUP Employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. This would prevent tarnishing the public image of CARNIVAL GROUP because when email goes out from CARNIVAL GROUP the general public tends to view that message as an official policy statement from the CARNIVAL GROUP.

## 2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at CARNIVAL GROUP. These rules are in place to protect the employee and CARNIVAL GROUP. Inappropriate use exposes CARNIVAL GROUP to risks including virus attacks, compromise of network systems and services, and legal issues. This policy also covers appropriate use of any email sent from a CARNIVAL GROUP Email address and applies to all employees & others workers (Contract workers & free lancers) on behalf of CARNIVAL GROUP.

## 3.0 Scope

This policy applies to employees & other workers (contract workers & free lancers) at CARNIVAL GROUP, including all personnel affiliated with third parties. This policy applies to all equipment that is owned by or leased to CARNIVAL GROUP & would be applicable from $1_{st}$ November 2015.

# Policy Index

## Password and PIN Security Policy

**Objective: Passwords and Personal Identification Numbers (PINs) used to Protect Business Critical Information must be properly structured, routinely changed, and kept strictly confidential.**

### Password/PIN Usage and Confidentiality

**[1]** All passwords and/or PINs must be handled as CARNIVAL GROUP Confidential, with additional requirements as specified below.

**[2]** Individual users must properly protect passwords and/or PINs for all accounts.

**[2.1]** Passwords and/or PINs unique to an individual must not be shared with other Individuals or users.

**[2.1.1] Exception:** Passwords may be shared with authorized diagnostic/help Desk personnel. After the authorized maintenance activity is completed, Diagnostic/help desk personnel must mark the password as expired, and the user must be required to change it at the first use.

**[2.2]** Use of group User IDs and their associated passwords is strongly discouraged and should be allowed only when necessary to support business processes.

**[2.3]** Writing down passwords or PINs is strongly discouraged and should be allowed Only when necessary to support business processes. Passwords or PINs that must be written down must be appropriately safeguarded to prevent disclosure to anyone other than their owner.

**[3]** Passwords/PINs must not be displayed on the screen at any time.

**[4]** Passwords and/or PINs must be changed whenever there is any indication of system or Password compromise.

**[5]** Any password or PIN management system either must avoid caching the password or PIN, or must provide adequate protections and controls if such caching is essential.

**[6]** Passwords and/or PINs must always be encrypted when held in storage or when transmitted across any network.

**[6.1]** **Exception:** One-time passwords or PINs, or hard-coded passwords or PINs that Meet the exception requirements below in paragraph [8.1], or passwords or PINs delivered in accordance with the applicable email delivery requirements in paragraph [26], or any passwords or PINs transported over a closed network (as defined in U.S. FDA regulations as requiring authentication and authorization for access) between two servers where logical and physical access to the servers is restricted to authorized users, the two servers are in close physical proximity such that traffic between them is over connections within the same physical area, the two servers are on the same logical subnet and thus serviced by the same switch, firewall or router, and the only individuals who may gain access to the passwords or PINs are system administrators who have privileged accounts on those servers.

**[6.2]** Use of a CARNIVAL GROUP approved hashing algorithm is considered Encryption for the purposes of password or PIN protection.

**[7]** Unencrypted passwords and/or PINs must never be embedded in sign-on utilities. For example, an unauthorized user must never be able to authenticate at sign-on merely by using a function key or by running an available program.

**[8]** Unencrypted passwords and/or PINs must not be hard-coded in source code, command files, initialization files, scripts or installation kits.

**[8.1]** **Exception:** Passwords and/or PINs may be placed in command files, initialization Files or scripts if access to such files is restricted to only those individuals responsible for administration of the system or application on which the files reside.

**[9]** PINs shall only be used where a numeric method for authentication is required (e.g., for entry on a telephone keypad); in all other instances, passwords should be used for authentication.

## Password/PIN Length

**[10]** Passwords and/or PINs must have a minimum length of six (6) characters.

**Exception:** For passwords or PINs meeting the exception requirements of Paragraph [8.1], they must contain a minimum of 8 characters.

## Password Complexity

**[11]** Passwords constructed using the Latin, Cyrillic or Greek alphabets must contain characters from at least three (3) of the following four classes (passwords constructed using Hindi characters have no complexity requirements):

### Class Description Examples

1. Upper Case Letters A B C … Z
2. Lower Case Letters a b c … z
3. Westernized Arabic Numerals 0 1 2 … 9
4. Non-alphanumeric (“special characters”, punctuation, symbols) { } [ ], < >; „“? / | \ ` ~ ! @#$ % ^ & * ( ) _ - + =

**[11.1] Exception:** Passwords may contain characters from fewer classes if their minimum Length is increased to provide overall security equivalent to eight Characters/ three classes.

**[12]** Passwords must not be derived from commonly used words or phrases.

**[12.1]** Users must be trained not to select passwords consisting of easily guessed Words, such as words found in dictionaries (English and non-English), User IDs, proper names or other names or words readily associated with the individual User, such as dates, nicknames and family names.

**[12.2]** Users must be trained not to select passwords consisting of easily guessed Words preceded and/or followed by one or more numbers or a special character. (For example, Daniel! $Roberto, $$Stew, 1Walt2, Ivy123, 321Bob and 4Shannon are not acceptable).

**[12.3]** Users must be trained not to select passwords, or PINs, that contain personally identifiable numbers, such as the users telephone extension, PAN Number, or zip code.

## Password/PIN Expiration

**[13]** Passwords and/or PINs must be changed at least every ninety(90) days.

**[13.1]** **Exception:** For passwords or PINs meeting the exception requirements of Paragraph [8.1], if the application owner has a compelling and documented business need, and has instituted data owner approved compensatory controls to ensure that such passwords or PINs are strongly protected, then those passwords and PINs need not be changed; otherwise, they must be changed at least once every 120 days.

**[13.2]** Temporary or initial passwords and/or PINs must be marked as expired when issued to a user, and the user must be required to change the password or PIN at the first use.

## Disabling of Accounts

**[14]** All accounts that provide access to Business Critical Information must be automatically locked out after three (3) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes.

## Default Passwords/PINs

**[15]** Any default password or PIN must be changed during or immediately upon the completion of the installation process. The new password or PIN must conform to the requirements defined in this policy.

**[16]** Default accounts must be renamed, if possible, to non-obvious names.

## Password/PIN Reuse

**[17]** User-chosen passwords and/or PINs must not be reused for five (5) iterations.

**[18]** Temporary passwords or PINs issued by a help desk or administrator to a user must be changed by the issuer on a daily basis and must not be reused for at least six (6) months.

**[18.1] Exception:** Re-use checks need not be done if random number generators are used to create the temporary passwords.

## Password/PIN Changes

**[19]** Proper proof of identification must be provided before changing a password or PIN.

**[19.1]** Users changing a password or PIN via a system command or screen must prove Knowledge of the current password or PIN or be cryptographically authenticated before being allowed to change it.

**[19.2]** The minimum time between user initiated password and/or PIN changes must be at least one (1) day. If a user has recently changed a password and is concerned that the new password may have been compromised, but is unable to immediately change it again in accordance with this provision, the user should contact an administrator of the system in which the password is used to affect a password reset.

**[19.3]** Users requesting a new password or PIN or requesting a password or PIN Change/reset via a help desk or administrator must prove their identity before the change is initiated.

**[19.3.1]** Acceptable forms of identification include:

- Company-issued ID card (presented in person to the administrator or a pre-established, trusted third party, such as a security guard)
- IT department call back the user after confirmation of details from HR department.

**[20]** The new or reset password or PIN must be delivered in accordance with the requirements documented below in Password/PIN Delivery.

**[21]** The new or reset password must be treated as a temporary password, as documented above in paragraph [13.2].

**[21.1]** The new or reset password must conform to the Password Length and Password Complexity requirements documented above.

**[22]** If a resigning or terminated staff member was responsible for system administration, then that individual's supervisor will ensure, commensurate with the risk, that all appropriate passwords are changed as soon as possible.

**[23]**

## Password/PIN Delivery

**[23]** Delivery of passwords and PINs to a user, either when an account is created or when an Administrator resets a password/PIN, requires attention to ensure that delivery is done efficiently and with a regard to security. Passwords must not be transmitted over any CARNIVAL GROUP voice, video or data network without appropriate identification and authentication.

**[24]** A User ID and associated password must not be delivered via the same medium at the same time (i.e., if the User ID is to be delivered by one medium, the password must be delivered by a different medium, or at a different time) except as allowed in paragraph [26].

**[25]** A password must be delivered in a manner that requires the recipient to prove his/her identity before the password is received. Acceptable delivery methods in descending order of preference are:

- **Person-to-Person,** after the user has presented his/her corporate ID card or a Government-issued, photo ID card, or is well known.
- **E-mail,** but only if:

1) The confidentiality of the message is protected using CARNIVAL GROUP 2) The message is delivered to a CARNIVAL GROUP email address that has been verified in a CARNIVAL GROUP Corporate Directory and is only transmitted over Intranet. Systems using this approach must also ensure, through technical enforcement, that the password is treated as a temporary or initial password as documented in paragraph [13.2].

**Telephone,** after the user has been authenticated by a previously established method, such as voice recognition or trusted party (e.g., an office security guard).

- **Company mail,** if, and only if, delivered in a sealed envelope to an address that is verified in a current CARNIVAL GROUP Corporate Directory, with confirmation of receipt.
- **Mail** (i.e., via the local postal service), if, and only if, the user is not located at a CARNIVAL GROUP facility. The information must be delivered in a sealed envelope, and the address must have been on file and not provided by the user. Confirmation of receipt is required.
- **Voice Mail**, to a user's PIN or password protected voice mailbox after the users telephone number has been verified in a current CARNIVAL GROUP Corporate Directory.

## Policy Enforcement

**[28]** Administrators are accountable for configuring systems to enforce this policy.

**[29]** Where possible, the system must enforce these requirements.

**[30]** Where this is not possible, equivalent controls must be established through alternative Methods or procedures. For example, to enforce password complexity, the Administrator should run tools periodically to detect weak passwords, and require users with weak passwords to change their passwords.

## Anti-Virus and Malicious Software Protection Policy

**Objective: CARNIVAL GROUP and computing resources shall be protected from malicious software code and viruses.**

## Scope:

**This policy applies to all computer systems that access or process CARNIVAL GROUP Information. All such CARNIVAL GROUP Owned or managed systems shall use approved software**.

## Definitions

Any reference in this document to a "**virus**" includes, but is not limited to, computer viruses, worms and malicious macros. Any reference in this document to "**spyware**" includes, but is not limited to, key loggers, screen capture programs, ad-ware and other malicious programs.

## Minimum Implementation Standards:

## Monitoring

**[1]** The monitoring, scanning and screening, and the quarantine/confiscation of any computing device must respect the privacy rights of users and will comply with all applicable laws and government regulations.

**[2]** CARNIVAL GROUP reserves the right to scan networking and computing resources for malicious Software, including but not limited to virus activity or spyware, at anytime, consistent with paragraph [1], and to monitor or screen content and traffic patterns including activity and traffic originating remotely. The purposes for such monitoring and/or screening includes, but is not limited to, system maintenance, detection and elimination of contamination, detection and prevention of unauthorized disclosures of CARNIVAL GROUP Business Critical Information, detection of unauthorized access to networking and computing resources, and determination of compliance with CARNIVAL GROUP Policies.

**[3]** CARNIVAL GROUP Reserves the right to quarantine and/or confiscate any computing resource that may pose a threat to CARNIVAL GROUP Including, but not limited to, data, Messages and network traffic. If such monitoring, screening, and/or quarantining reveals possible evidence of criminal activity, appropriate action will be taken which may include, among others, providing evidence from the monitoring/scanning/screening to law enforcement officials.

**[4]** CARNIVAL GROUP Reserves the right to immediately disconnect, without prior notification, any device found inadequately protected by approved or accepted anti-virus or anti-spyware software. Devices thus removed from the network must demonstrate Policy compliance including current anti-virus and anti-spyware software, signatures, and configuration prior to any reconnection to CARNIVAL GROUP.

## Anti-Virus Software Requirements

**[5]** Servers, desktops, laptops, workstations and PDAs shall have commercial anti-virus software installed, properly configured and running at all times (i.e., never disabled during normal operation).

**[5.1]** For servers offering file and print, collaboration, groupware, FTP and e-mail services, and which process CARNIVAL GROUP Information or access CARNIVAL GROUP resources:

**[5.1.1]** Operating Companies should employ, where possible, servers that run Operating systems that have SSB-prescribed anti-virus software;

**[5.1.2]** **Where** an operating system (Apple Mac OS) must be used for which there is no prescribed Anti-virus software, the Operating Company shall:

- determine whether there is acceptable anti-virus software available commercially and if so, propose that CARNIVAL GROUP Review and approve its use.

- Implement other measures in the absence of such anti-virus Software to reduce the likelihood of a virus infestation; otherwise the device must be isolated from the Internet.
- Note: if there is an operating system capable of being infected by a virus, Trojan, or other malicious software then it MUST be patched in accord with **Information System**

**Administration and Management Security Policy** (paragraph [12]), and have Antivirus software installed as Specified in this policy.

**[5.1.2.1 ] Exception:** If there is any customized software being used for business need and it has been advised not to use Anti-virus software for the same, IT head must ensure that system details are documented and all recommended patches are updated before deployment. Such systems/servers must be under 24 hour’s vigilance and if possible Internet access must be blocked on them.

**[5.2]** If present, the “heuristic” scanning property of anti-virus software must be enabled.

**[5.3]** Anti-virus software must be configured to automatically clean the infected file, (i.e. Remove the virus) or quarantine or deny access to the infected file if automatic cleaning is not possible.

**[5.4]** Users shall not disable automatic virus scanning.

**[5.4.1] Exception:** With the approval of the IT- Head, brief disablement to allow Installation of authorized software is permitted for the duration of the installation. If the approved software has been downloaded from a public network (e.g., the Internet), the device must be disconnected from CARNIVAL GROUP prior to disabling the anti-virus software. Automatic virus scanning shall be re-enabled immediately after the installation is completed, and a complete system scan done prior to reconnecting to CARNIVAL GROUP. The IT Head shall ensure that there is a written process or procedure to verify that the automatic virus scanning has been re-enabled, and shall ensure that process or procedure is followed.

**[5.5]** Server Administrators shall not disable anti-virus software.

**[5.5.1] Exception:** With the approval of the IT Head, brief disablement to allow troubleshooting a problem is permitted. The server administrator shall ensure that there is a written process or procedure to verify that the antivirus software has been re-enabled, and shall ensure the process or procedure is followed.

## Anti-Virus Scanning

**[6]** The following tables contain the rules for scanning files. Only local drives (e.g., hard disk, CD, ZIP drive, and USB drive) and local content may be scanned by users. Users shall refrain from scanning network resources.

| | **Desktop /Laptop / Workstations/ PDA** | **File and Print Servers** | **Application, Collaboration, Groupware Servers** | **E-mail and FTP Servers** |
|---|---|---|---|---|
| **Weekly** | All local drives ALL Files | All local drives & hosted drives ALL Files | All local drives ALL Files | All local drives ALL Files |
| **On-Access (read from** | Default Files | | | ALL Files |

| | | | | |
|---|---|---|---|---|
| **disk)** | | | | |
| **On-Storage (Write to disk)** | Default Files | Default Files | Default Files | ALL Files |
| **Electronic mail Scan** | Incoming Message<br>& Attachment | Incoming Message<br>& Attachment | Incoming Message And Attachment | Incoming & Outgoing Message and Attachment |

**[7]** All electronic mail entering and leaving CARNIVAL GROUP (i.e., to/from the Internet, or to/from a Business Partner, or vendor) must be scanned.

**[8]** The scans cited above must occur without user initiation or intervention.

**[9]** Electronic mail entering or leaving CARNIVAL GROUP may be blocked on the basis of subject or body text phrases

**[10]** Attachments that are part of electronic mail entering or leaving CARNIVAL GROUP may be blocked. Attachment blocking is done primarily on the basis of the file extension of the attachment, but blocking may also be based on (parts of) file names or file size. The list of blocked items is maintained by CARNIVAL GROUP and shall be reviewed periodically and updated, as circumstances require.

**[11]** Security related scans settings for laptops, desktops, workstations, and the CARNIVAL GROUP IT department shall determine PDAs that are not explicitly addressed by this policy.

**[12]** Electronic messages with questionable or suspicious subject lines or content must be deleted without opening, regardless of the origin of the message. Users shall not open any files attached to electronic mail from unknown, suspicious or un-trusted sources.

## Anti-Virus Updating

**[13]** Site Administrators are responsible for validating version, engine and signature files for Desktop/Laptops and PCs; Server Administrators have this responsibility for servers. Users have this responsibility for stand-alone PCs and laptops that are never connected to the network.

**[14]** Whenever possible, signature and engine updates must be installed without user initiation or intervention.

**[15]** New versions of the virus signature files must be loaded as soon as possible, but no later than **one (1) week** after release by the vendor. Failure to perform this within **one (1) week** may result in disconnection from CARNIVAL GROUP.

**[16]** New security patches for the current anti-virus software package must be installed consistent with **Information System Administration and Management Security Policy** (paragraph [12]).

**[17]** New releases of the anti-virus scanning engine must be installed as soon as possible, but no later than **four (4) weeks** after release by the vendor. Failure to perform the installation within **four (4) weeks** may result in disconnection from CARNIVAL GROUP.

## Virus Reporting

**[18]** Users must notify the local help desk whenever a computer virus is suspected or detected.

**[19]** Where the software supports virus alerting, all virus detections must be automatically and immediately reported to personnel directly responsible for the infected device. The alerts must also be forwarded to the Regional Support Center and/or Regional Service Center as directed by CARNIVAL GROUP.

**[20]** All virus alerts must be followed by an immediate and complete scan of affected devices, performed by qualified personnel. "Virus alerts" include, but are not limited to, user calls about problems that may be virus related and triage indicates that a "virus alert" is warranted, network monitoring, reporting evidence of virus related behavior (e.g., network sweeping, suspicious/irregular use of ports, etc.), and anti-virus software automatic warnings to alert qualified personnel as to the detection of a virus.

**[21]** Site administrators must ensure a root-cause investigation is conducted when a virus is identified on a computing device for which the administrator is responsible.

## Anti-Spyware Software Requirements

**[22]** Laptops, desktops, and workstations shall have commercial anti-spyware software installed, properly configured, and running at all times.

**[22.1]** If present, the behavioral based detection capability of the anti-spyware software must be enabled.

**[22.2]** Anti-spyware software shall be configured for on-access scanning to detect and Block unwanted programs before they are installed.

**[22.3]** Anti-spyware software shall be configured to automatically remove malicious or unwanted programs, or quarantine them if automatic removal is not possible or advisable.

**[22.4]** Anti-spyware software shall be configured to scan all local drives weekly.

**[22.5]** Users shall not disable spyware scanning.

**[23]** New versions of spyware signatures must be loaded as soon as possible, but no later than **one (1) week** after release by the vendor. Failure to perform this within **one (1) week** may result in disconnection from CARNIVAL GROUP.

**[24]** New releases of the anti-spyware scanning engine must be installed as soon as possible, but no later than **four (4) weeks** after release by the vendor. Failure to perform the installation within **four (4) weeks** may result in disconnection from CARNIVAL GROUP.

**[25]** Whenever possible, anti-spyware signature and engine updates must be installed without user initiation or intervention.

**[26]** Site administrators are responsible for validating anti-spyware version, engine, and signature files. Users have this responsibility for stand-alone laptops, desktops, and workstations that are not connected to the network.

**[27]** New security patches for anti-spyware software shall be installed consistent with Information **System Administration and Management Security Policy** (paragraph

## Personal Firewall Software Requirements

**[28]** Laptops, desktops, and workstations shall have a CARNIVAL GROUP approved software firewall installed and operating in accordance with the following requirements:

**[28.1]** The firewall shall be configured to block all inbound traffic other than that required for business purposes.

**[28.2]** The configuration of the firewall shall not be capable of being modified or updated at any time by any unauthorized personnel, including as appropriate the end user.

**[28.3]** The configuration of the firewall shall be further updated at any time by CARNIVAL GROUP in response to prevailing threat conditions.

**[29]** Firewall logs and events shall be available for analysis by CARNIVAL GROUP security operations for evaluation of current threat conditions and to confirm that the firewall is correctly configured and operating properly over time.

**[30]** Site Administrators are responsible for ensuring the firewall is implemented on all Operating Company laptops, desktops, and workstations.

The Portion is intentionally left Blank

## Information System Administration and Management Security Policy

**Objective: CARNIVAL GROUP System administration security practices must ensure that all CARNIVAL GROUP Information systems are always in a known, secure state, those information resources are properly documented and accounted for and that their use is controlled and protected.**

## Minimum Implementation Standards:

### General

**[1]** This policy applies to all assets, both hardware and software, used to create, transfer or store information for use by or for CARNIVAL GROUP.

**[1.1]** Hardware – Servers, desktop computers, laptop computers, PDAs, routers, switches, hubs, etc.

**[1.2]** Software – Server/Client and business application software and its original documentation.

### Documentation

**[2]** Each Operating Company and Operating unit must maintain a database for hardware and software assets noted above used within or owned by that entity.

**[3]** The owner of the asset must control all original documentation for CARNIVAL GROUP assets.

**[4]** CARNIVAL GROUP information system assets must have the following information recorded in a database for use in tracking and control:

**[4.1]** Description – what is the asset (server, computer, software, etc.);
**[4.2]** Brand, make, model;
**[4.3]** Owner – who is responsible for the asset;
**[4.4]** Purpose – asset's intended use;
**[4.5]** Unique Identifiers – serial number, version number, MAC address, IP address, Bar code; and
**[4.6]** Location – specific location of asset (building, room number).

**[5]** Each Operating Company and Operating Unit must document the configuration of each computing and network asset. The documentation must contain, but not be limited to:

**[5.1]** Unique Identifier

**[5.2]** Operating system (OS)

- Version
- Patches and date(s) of patch

**[5.3]** Listing of software titles installed on platform

- Version
- Patches and date(s) of patch

**[5.4]** **Internal** Peripherals (modems, network interface cards, etc.)

- Make and model
- Software driver version

**[6]** No server may be connected to CARNIVAL GROUP without first being registered with the DNS (Domain Name Server) and being entered into the asset database.

**[7]** Software other than standard:

**[7.1]** If other-than-standard software is required to perform an employee's duties, authorization from his/her manager is required.

**[7.2]** Any other-than-standard software must be evaluated by the IT department to ensure that it is compatible with CARNIVAL GROUP and all associated Policies.

**[8]** Administrators must maintain tables, diagrams and other records of baseline system and Security configurations, and any configuration changes for all hardware and software system components. Documentation requirements may include:

**[8.1]** **Security** configuration for operating systems, client/server, legacy and stand-alone applications, infrastructure equipment (router, switch, premise), and security servers (Firewall, PKI, intrusion detection, authentication server, etc.).

**[8.2]** **Contact** information for all individuals and organizations that may contribute to System support (e.g. name, address, telephone number, pager number, e-mail, service/product/expertise, etc.). This includes system administrators, managers, communications service providers, expert consultants, maintenance and technical support contractors and equipment and software vendors.

**[8.3]** Special information, such as customer ID number, PIN, circuit and port numbers, account number, etc., that may be needed when contacting support personnel.

**[8.4]** Passwords for all administration-related accounts and equipment/systems (firewall, router, service accounts, and administrator accounts).

**[8.5]** LAN/WAN architecture diagrams with references to physical locations.

**[8.6]** IP/IPX/SPX address plan with address allocations.

**[8.7]** Server operating system services (domain controllers, WINS, DNS, DHCP, print, file, Remote administration, etc.) And how and where they are installed.

**[8.8]** Application software services (messaging, database, Web, tape backup, security, etc.) and how and where they are installed.

**[8.9]** **Router** configuration and routing tables.

**[8.10]** Premise equipment configuration.

**[8.11]** Location of vendor manuals (hardcopy and electronic) for commercial hardware and software products.

**[8.12]** Hardware inventory with type, model, purpose and location.

**[8.13]** Software inventory with version, patch level, installation options, purpose, location, license numbers and keys.

**[9]** Information listed above must be maintained in multiple, protected, locations to guarantee its availability when needed, while preventing its disclosure to all but authorized personnel.

## Configuration Management

**[10]** Standard Software Configurations

**[10.1]** Standard configurations must be documented for, but not limited to, the following:

- Microsoft Windows Operating Systems (9.x, NT, Win 2000, XP)
- UNIX/LINUX Operating System
- Mac Operating System

- Domain Controllers
- Data base Servers
- Email Servers
- Application Servers
- Standard Desktop Computers
- Standard Laptop Computers
- Routers
- Multi-Function Devices (e.g., printers, faxes, scanners)

**[10.2]** Configurations must include any modification that is not made by the "out of the box" default install (e.g., IP address of a server).

**[10.3]** Configurations must include any security-related modifications.

**[10.4]** Configurations must be approved by IT Head.

**[11]** Security configuration must be consistent with applicable CARNIVAL GROUP standards.

**[11.1]** Administrators are accountable for configuring systems to ensure compliance with this policy.

## Security Patches and Software Updates

**[12]** Administrators must regularly monitor applicable sources for information regarding security bulletins or the release of security software patches.

**[12.1]** Administrators must apply all system and security patches (service packs, hot fixes, patch clusters, etc.) in accordance with the schedule below after they have been tested and approved. Administrators must document the baseline configuration. Documentation must include the equipment/software affected, the patches applied, their versions, their Purposes, where they were obtained, installation procedures and any subsequent configuration changes.

**[12.2]** Security patches must be implemented as soon as possible (ASAP), but no later than required by the following schedule:

- **Critical:** As determined by the IT Head & Security Managers, but No later than seven (7) calendar days after release by the vendor. IT must make the patch available prior to the designated implementation timeline, but no later than **three (3) calendar days** after release from the vendor.

- **High:** Within **thirty (30) calendar days** after release by the vendor, of which IT has **seven (7) Calendar days** to make it available for installation.

- **Medium:** Within **ninety (90) calendar days** after release by the vendor of Which IT has four

**(4) Weeks** to make it available for installation.

- **Low:** Within **one hundred and eighty (180) calendar days** after release by the vendor of which IT has **four (4) weeks** to make it available for installation.

**[12.3]** The determination that a patch is critical will be made by the IT Head based on recommendations from System administrators.

**[12.4]** When patches that have been assigned different ratings are released from the Vendor in a bundle (e.g., service pack) and cannot be implemented independently, the implementation schedule for the IT Head will make the bundle jointly.

**[12.5]** If a system is connected to CARNIVAL GROUP and the information owner determines that there is a compelling business reason that precludes meeting these patching requirements, then the system and its connection must be evaluated for appropriate security, documented, initiated by IT Head and approved by the CEO.

**[12.6]** If security patches for software, including but not limited to operating systems, databases, and applications, are no longer available because the vendor has discontinued support, Operating Companies or Operating Units that use this software must take the following measures:

**[12.6.1]** Identify and document the systems that are using the unsupported software and submit the documentation to IT Head.

**[12.6.2]** If the systems are connected to CARNIVAL GROUP, consult with IT to determine what approaches can be used to ensure adequate risk mitigation for CARNIVAL GROUP.

**[12.6.3]** Obtain concurrence from the IT Head that a particular approach is acceptable, and if so, what security mechanisms and specific configuration settings must be used to support the approach.

**Exception:** If the implementation of an appropriate risk mitigation approach is not possible for technical or financial reasons, the IT Head must approve the use of the systems. Approval of Head of Operations represents acknowledgement that the systems may be denied access to, or removed from CARNIVAL GROUP, should the system represent a significant risk. The determination that a particular threat or vulnerability constitutes a significant risk will be made by the IT Head.

**[13]** Administrators must regularly monitor the Internet and other information sources for security advisories that pertain to constituent system products.

**[14]** Software updates and patches

**[14.1]** Software updates and patches must be researched, tested and verified by appropriate personnel before installing on any CARNIVAL GROUP asset.

**[14.2]** Only applicable updates and patches may be applied to corporate assets.

**[14.3]** Updates for common software titles used by CARNIVAL GROUP must be made accessible to all users of CARNIVAL GROUP after testing has been completed.

**[14.4]** Software updates and patches must only be acquired from the approved CARNIVAL GROUP location.

**[14.5]** A list of approved software packages and version numbers for use on computers connected to CARNIVAL GROUP must be posted and made accessible to all users of CARNIVAL GROUP.

**[14.6]** Software updates for custom applications should be installed only after testing and Verification from Vendors related to all the integration and should be deployed as per other CARNIVAL GROUP policies and verification/confirmation by the user department.

## Warning Notice

**[15]** All CARNIVAL GROUP computers and network control devices (e.g., router, switch, hub) that Provide access to must display a legal notice/warning message to deter theft of data:

**[15.1]** All CARNIVAL GROUP computers that provide access to must display the following legal notice/warning message to deter theft of data:

**"WARNING NOTICE:** You are about to enter a Private Network that is intended for the authorized use of a Private Company and its affiliate companies (the "CARNIVAL GROUP ") for business purposes only. The actual or attempted unauthorized access, use, or modification of this network is prohibited by the Company. Unauthorized users and/or unauthorized use are subject to Company disciplinary proceedings and/or criminal and civil penalties in accordance with applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons. If such monitoring and/or recording reveal possible evidence of criminal activity, the Company may provide the monitored evidence of such activity to law enforcement officials."

The message must precede the login process, when possible.

**[15.2]** All CARNIVAL GROUP Control devices that provide access to CARNIVAL GROUP must display the following legal notice/warning message, prior to login, to deter theft of data:

**"WARNING NOTICE:** This is a private system. The actual or attempted unauthorized access; use or modification of this system is strictly prohibited. Individuals undertaking such unauthorized access, use or modification are subject to company disciplinary proceedings and/or criminal and civil penalties under applicable domestic and foreign laws. The use of this system may be monitored and recorded for administrative and security reasons in accordance with local law. If such monitoring and/or recording reveal possible evidence or criminal activity, the results of such monitoring may be provided to law enforcement officials. Continued use of this system after receipt of this notice constitutes consent to such security monitoring and recording."

**[15.3]** All CARNIVAL GROUP control devices must display the following legal Notice/warning message, after login, to deter theft of data:

**"WARNING NOTICE:** This is a private system for use by CARNIVAL GROUP and its affiliates. If you are not an authorized user of this system disconnect immediately**."**

## Periodic Maintenance

**[16]** Administrators must use tools and procedures to evaluate configuration and verify functionality and integrity of security services.

**[16.1]** Tools must be actively supported so that frequent updates are available.

**[16.2]** Tools must support both automated and on-demand use.

**[16.3]** Administrators must disable or delete all inactive user accounts.

**[16.3.1]** User accounts must be disabled immediately upon an individual's termination of employment or termination of a business relationship with CARNIVAL GROUP.

**[16.3.2]** New accounts that remain unused for seven (7) days must be disabled.

**Exception:** Excluding network and remote access accounts, the timeframe for disabling new accounts that remain unused may be extended to forty-five (90) days with IT Head's approval.

**[16.3.3]** Any account not accessed for more than forty-five (45) days must be disabled.

**Exception:** This requirement does not apply to local administrative accounts (i.e., local to the machine on which they exist) that are required to be present but that are rarely accessed locally and never accessed over the network.

**[16.3.4]** Any disabled account not requesting reactivation within 370 days must be deleted.

**Exception:** This requirement does not apply if deleting the account would cause a noncompliance with governmental regulations.

## Asset Protection

**[17]** Administrators must ensure that anti-virus software is installed and updated in accordance with **Anti-Virus and Malicious Software Protection Policy.**

**[18]** Users must not leave computer terminals unattended. Use of password-protected or token protected, user authenticated screen-saver programs is mandatory. The screen saver must be invoked after a period of no longer than 5 minutes of no user activity.

**[19]** Where appropriate, access rights to information systems or computing resources must support a mechanism that provides for segregation of duties. In order to limit the potential for fraud or system compromise, account authorization rights and application/transaction capabilities must not be granted to the same individual.

**[19.1]** Where business requirements or application limitations demand granting access Rights that compromise the principle of segregation of duties, approved management controls to mitigate the assessed risk must be implemented, documented and monitored.

**[19.2]** Where segregation of duties is implemented, access control lists must be reviewed At least quarterly.

**[20]** Administrators must grant users only the privileges necessary to perform their duties (i.e. least privilege needed for that purpose).

**[20.1]** Only the individual resource owner may grant additional access rights and privileges.

**[20.2]** The management responsible for the resource must approve the granting of administrator access rights and/or privileges or the creation of an account with any administrator privileges. The number of administrator accounts must be limited to the minimum number required to effectively manage and operate the resource. The business rationale for these accounts and the procedures for controlling their use must be documented, reviewed and reauthorized at least annually.

**[21]** Local administrative privileges on workstations (desktops and laptops) must be limited and controlled to prevent possible compromise of the device. Operating Companies must document a business need before granting local administrator privileges to an individual or group of workstation users. A consistent rationale must be employed that considers an individual's job function. These procedures should be re-examined and re-approved at least annually.

**[22]** Physical access to all servers and networking/internetworking premise equipment must be restricted to authorize personnel only.

**[23]** Administrators must protect account information that resides on authentication servers (e.g., a Microsoft Windows primary or backup domain controller).

**[23.1]** In a Microsoft Windows environment, this would include protection for Emergency Repair Disks, Security Account Management database access, registry access, password hashes, and Local Security Authority database access.

**[23.2]** In a UNIX/MAC environment, this would include password and shadow password files.

**[24]** Data must be backed up periodically to a removable storage medium, to maximize availability and prevent information loss in the event of a problem.

**[24.1]** Data must be backed up periodically and include both business data (e.g. database, files, e-mail, etc.) and system data (e.g., Emergency Repair Disk, router configuration files, firewall configuration files, scripts and utilities, etc.).

**[24.2]** Besides scheduled, periodic backup, business and system data must be backed up immediately prior to any system upgrade or maintenance activity that could result in a system failure.

**[24.3]** Backup data must be stored off-site at a specialized, secure facility designed for that purpose.

**[24.4]** The process of restoring data from tape or other media must be tested at least quarterly to ensure the integrity of the storage media, equipment, software and staff proficiency.

## Log/Monitor/Audit

**[25]** Administrators must provide logging and auditing functions for system security events related to logon/logoff, creation of accounts, access privileges, user rights, permissions, group membership, unauthorized access attempts, account lockouts, security policy and process tracking. Log files must be maintained for not less than ninety (90) days.

**[25.1]** Event information must include, at a minimum: date, time, source (user, system or process) and description.

**[25.2]** Logging and auditing must occur on all servers, internetworking equipment and Access control devices that support them.

**[25.3]** Automated synchronization to a trusted centralized time standard must be configured on all servers, internetworking equipment and access control devices that support it.

**[25.4]** Log files must be protected from accidental or intentional modification or destruction. Administrators must utilize enterprise tools for management of log files. The tools must include functions for automation, analysis, reporting, access control, distribution, and storage management.

## Incident Response

**[26]** Administrators must report and respond to security events or suspicious activity in accordance with the CARNIVAL GROUP Policies**.** All accounts that process or access Business Critical Information must be automatically disabled after five (5) sequential invalid login attempts within a fifteen (15) minute period. After being disabled, the account must remain locked out for a minimum of fifteen (15) minutes.

## Loss of Corporate Asset

**[27]** Any loss of or damage to a corporate asset must be reported to the owners manager, the Local IT staff, and the local Operating Company Chief Information Security Officer as soon as possible but not later than 24 hours after detection of the loss.

**[27.1]** The loss of or damage to a computing device must be reported and a Damage Assessment Report filed in accordance with **Portable Computing Device Security Policy.**

**[28]** When good judgment and /or due diligence & care has not been exercised in safeguarding an asset, the individual may be subject to disciplinary action and held responsible for the replacement cost if the asset is lost or stolen. The decision of the IT Head in this regard shall be final and conclusive.

## Asset/Information Disposal

**[29]** When business requirements dictate, computing assets and/or portable storage devices must be properly disposed. Disposal of these devices must follow written standards that each company is responsible for developing. However, in the case of computing devices with storage capabilities or portable storage devices each potentially containing CARNIVAL GROUP Business Critical Information, extreme care must be exercised when disposing of these devices. The following areas must be adequately addressed during the disposal process:

**[29.1]** Disposal of computing and storage devices should be managed by e-waste policy.

**[29.2]** All equipment that contains or could have contained Business Critical Information Must be checked to ensure that all such information has been backed up or retained elsewhere, if appropriate, and removed prior to disposal.

**[29.3]** If the Operating Company elects to contract with a third party for the actual disposal, the Operating Company must ensure there is comprehensive Non-Disclosure Agreement language included in the Work Agreement prior to commencement of disposal services in order to protect Business Critical Information from unauthorized disclosure. The third party should provide the Operating Company with a written statement of disposal detailing and documenting the work completed.

## Other Requirements

**[30]** The use of internal firewalls is permissible and encouraged. Their use and configuration is subject to the provisions of **Access Control Policy.**

**[31]** Random asset inspections must be made to verify location and condition of assets.

**[32]** Administrators must configure and maintain all systems in accordance with **CARNIVAL GROUP Information Asset Protection Policies.**

**[33]** All administrators must be adequately trained in the systems for which they are Responsible. Local management must maintain certification of completion of training.

**[34]** Configuration of network connected Multi-Functional Devices (MFDs) must comply with The following requirements:

**[34.1]** Multi-Function Devices that support multiple network interfaces must be configured To prevent unauthorized bridging between the interfaces except for the purpose of receiving and transmitting faxes.

**[34.2]** Images copied to a local hard disk or temporary storage file or media must be Erased or overwritten immediately upon completion of the action requiring the write.

**[34.3]** Multi-Function devices that have operating systems which are vulnerable to Infection by virus, Trojans, or other malicious code must have CARNIVAL GROUP-Approved Anti-Virus software, as specified in **Anti-Virus and Malicious Software Protection Policy,** installed and running at all times**.**

**[34.4]** If the device supports a transaction audit trail, this capability must be enabled.

**[34.5]** Network administrators are responsible for network configurations, and for determining the location of the device on the network based on the security capabilities of the device.

**[34.6]** Device configuration and maintenance through a network or dial-up interface is permissible, but must be controlled through the use of a password or token based access control function that meets the requirements of **Password and PIN Security Policy.**

**[34.7]** Remote diagnostic access must be disabled as the default condition. Activation of This capability must be managed in accordance with this policy.

**[34.8]** Where provided, logging of diagnostic events must be enabled.

The Portion is intentionally left Blank

## User Responsibilities Policy

**Objective: All users of computing resources and networks, who have access to CARNIVAL GROUP Business Critical Information, must comply with CARNIVAL GROUP Information Asset Protection Policy.**

## Introduction

This Policy is essentially a compilation of user-oriented requirements from all the other policies. It is presented for the convenience of the user.

## Minimum Implementation Standards:

### Information Protection Responsibilities

**[1]** All CARNIVAL GROUP employees, contractors, consultants, vendors and Business Partners are responsible and accountable for safeguarding and monitoring information assets against unauthorized disclosure, modification, destruction or loss of availability.

**[2]** Users must follow the access and handling requirements identified in local information security policies.

**[3]** Business Critical Information stored within a computer must be protected either by approved cryptographic protection or through appropriate physical protection of the computer, or both.

**[4]** Business Critical Information stored on removable storage devices, e.g., ZIP disks, USB tokens/pens, must either be encrypted using approved encryption, or must be physically controlled and protected against loss, theft, and unauthorized access.

**[5]** Personally Identifiable Information stored on desktop computers, laptops and other portable computing devices, or removable media that is classified as "Special Personal Data" by the Corporate Office of Privacy must be encrypted using cryptography.

**[6]** Processing Paper Documents with Business Critical Information.

**[6.1]** Paper documents containing Business Critical Information must be filed or locked away when not in use.

**[6.2]** When faxing sensitive Business Critical Information, the recipient should be called in advance and asked to take appropriate steps to ensure the fax is properly managed upon receipt.

**[6.3]** When finished using printers and fax machines, care must be taken to remove all paper documents. If the device stores an electronic copy of the document, and the document is sensitive, it should be deleted from its memory.

**[6.4]** All un-needed documents shall be destroyed in a proper manner.

**[7]** Only CARNIVAL GROUP -approved remote access devices may be used to access remote access services. Any device used to access remote access services must conform to the CARNIVAL GROUP **Information Asset Protection Policies (IAP)**.

**[8]** All CARNIVAL GROUP -owned remote access software and hardware must be returned upon a user’s end of employment or the completion of the need for remote access.

**[9]** Users remotely accessing CARNIVAL GROUP must be authenticated using strong authentication mechanisms.

**[10]** Any CARNIVAL GROUP computing device connected directly to any non-CARNIVAL GROUP (including, but not limited to the Internet) must be protected by a personal firewall on that device, configured and operating consistent with **Anti-Virus and Malicious Software Protection Policy** (paragraph [26]).

**[11]** CARNIVAL GROUP reserves the right to monitor content and traffic (including activity and traffic originating remotely), and to electronically screen networking and computing resources for all activity using CARNIVAL GROUP electronic messaging, or network and computing resources. The purposes of this monitoring and/or screening include the determination of compliance with all CARNIVAL GROUP policies. Such monitoring and/or screening will respect the privacy rights of users, including compliance with national or local laws.

**[12]** Users are required to respect the privacy of all individuals and organizations when they use the Internet.

**[13]** Users must not intentionally seek personal information, obtain copies of software, files, data or passwords belonging to Internet users, or represent themselves as someone they are not.

**[14]** Users must not intentionally modify or delete software, files, data or passwords of other users, unless explicitly authorized to do so by that other user/IT department.

**[15]** In order to obtain private information or other resources on the Internet that are not freely accessible to the general public, permission must be granted by the owner(s) or holder(s) of rights to that information or other resources. Attempts to access private information or other nonpublic resources on the Internet without obtaining proper approval are prohibited.

**[16]** A list of blocked content over CARNIVAL GROUP will be maintained in accordance with previous policies.

## Confidentiality Agreement

**[16]** All CARNIVAL GROUP personnel with access to CARNIVAL GROUP Business Critical Information assets must sign a confidentiality agreement which forbids the disclosure of such Information to parties within or outside of CARNIVAL GROUP who do not have a business need to know the information.

**[17]** All non-CARNIVAL GROUP personnel (temporary contract employees, contractors, Vendors/consultants and/or the vendor/consultant Company on their behalf, and third party users) must sign a nondisclosure agreement to receive access to any CARNIVAL GROUP Business Critical Information.

**[18]** Confidentiality and/or nondisclosure agreements must be reviewed periodically, and/or whenever there are changes in terms of employment or the contractual agreement.

## User Security Training

**[19]** A record must be maintained that every person with access to CARNIVAL GROUP business information acknowledges that he/she:

**[19.1]** Has read and understands the IT policies.

**[19.2]** Understands his/her responsibilities to comply with the policies which affect that person's job responsibilities.

**[19.3]** Understands the consequences of a violation.

**[20]** A security training and awareness program, including local information security policies must be:

**[20.1]** Provided as part of orientation upon initial access to CARNIVAL GROUP business information.

**[20.2]** Updated no less frequently than once per year via an awareness briefing.

**[20.3]** Documented to include records of security training and awareness.

## Electronic Messaging

**[21]** Users access to electronic messaging, telephonic communication, and networking and computing resources for business communications with other CARNIVAL GROUP entities or with other users is permissible.

**[21.1]** Users access, and the privileges associated with such access, must be limited to those needed for performing job requirements.

**[21.2]** Use of the auto-forwarding feature of CARNIVAL GROUP electronic messaging to email addresses other than those within the CARNIVAL GROUP internal e-mail system is prohibited.

**[21.3]** A user's non-CARNIVAL GROUP personal e-mail account (i.e. not residing on CARNIVAL GROUP) may not be used for CARNIVAL GROUP business unless management determines that there is a compelling business need to do so, and in any case, it may not be used to receive or process Business Critical Information.

**[22]** Electronic messages with questionable or suspicious subject lines or content must be deleted without opening, regardless of the origin of the message. Users shall not open any files attached to electronic mail from unknown, suspicious or un-trusted sources.

**[23]** Use of CARNIVAL GROUP electronic messaging, telephone communications, and networking and computing resources for transmission or distribution of inappropriate or offensive material, such as racial, religious, creed or gender slurs, or obtaining or distributing pornographic or sexually oriented materials is prohibited.

**[24]** CARNIVAL GROUP electronic messaging, telephonic communications, and networking and computing resources must not be used as means to interfere with or disrupt other users, services, or equipment. Disruptions include, but are not limited to, distribution of "SPAM", or propagation of malicious software.

**[25]** Remote access to CARNIVAL GROUP information systems over public workstations is not permitted. Public workstations include, but are not limited to, cyber cafes, Internet kiosks in airports or other public places, and terminals in public libraries.

**[25.1]** Users remotely accessing CARNIVAL GROUP must be authenticated using strong Authentication mechanisms.

**[25.2]** Only CARNIVAL GROUP -approved remote devices may be used to access remote access services. Any device used to access remote access services must conform to the CARNIVAL GROUP Information Asset Protection Policies.

**[25.3]** Users must disconnect from the remote access connection when not actively using it.

**[26]** Transmission of Business Critical Information:

**[26.1]** Business Critical Information must be protected and secured during any electronic Data transmission or electronic or physical media transfer.

**[26.2]** Business Critical Information may be transmitted electronically over CARNIVAL GROUP without encryption, although it is strongly encouraged that approved encryption is used when it is available.

**[26.3]** Business Critical Information **may not** be transmitted over a public network (such As the Internet) unless it is in an approved, encrypted form.

## Internet

**[27]** The Internet must not be used to communicate CARNIVAL GROUP Business Critical Information unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.

**[28]** Use of the Internet with CARNIVAL GROUP computing resources for recreational games, or for obtaining or distributing pornographic or sexually oriented materials, or for obtaining or distributing any materials inconsistent with CARNIVAL GROUP Credo, ethics and values, is strictly prohibited and any violation of this will be invite punitive action by the CARNIVAL GROUP management.

**[29]** Users are required to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used or obtained via the Internet using CARNIVAL GROUP computing resources.

**[30]** CARNIVAL GROUP computing resources must not be used as a means to interfere with or disrupt Internet users, services or equipment.

**[30.1]** Disruptions include, but are not limited to, distribution of “SPAM”, or propagation of malicious software.

**[30.2]** Using CARNIVAL GROUPcomputing resources to make or attempt unauthorized entry to any network or computer accessible via the Internet is prohibited.

**[31]** Downloading of non-CARNIVAL GROUP executable software and copyrighted materials (legal protections provided by patents, copyrights, trademarks, and intellectual property rights) using the Internet is strongly discouraged for security and legal reasons.

**[32]** Downloading of copyrighted materials will only be performed with management approval.

## Network and Computing Resources

**[33]** Networking and computing resources include, but are not limited to, electronic mail (email), voice mail, audio and video conferencing, facsimile, telephone, Internet services, computer hardware and software, network hardware and software, printers, copiers and other printed or electronic media.

**[34]** CARNIVAL GROUP encourages use of these networking and computing resources in imaginative and innovative ways, provided such use benefits CARNIVAL GROUP or its employees, in general, and does not involve non-CARNIVAL GROUP related personal gain or activities contrary to CARNIVAL GROUP principles, ethics and values and/or policies.

**[35]** Users must be positively and individually identified and authenticated prior to being permitted access to any CARNIVAL GROUP computing resource.

**[36]** Personal use of CARNIVAL GROUP electronic messaging, telephone communications, and networking and computing resources is permitted if such use is incidental and insignificant and it does not interfere with normal work activities. Any personal use:

- Must not involve solicitation;
- Must not be associated with any political entity.
- Must not promote any outside business activity.
- Must not potentially harm the reputation of CARNIVAL GROUP.
- Must not potentially expose CARNIVAL GROUP and/or its businesses to any liability, civil or criminal.

**[37]** The use of CARNIVAL GROUP electronic messaging, telephonic communication, and networking and computing resources for the following purposes is prohibited:

- Personal profit;
- Personal business;
- Personal political purposes;
- Antisocial or unethical behavior;
- Activities that violate international, country, federal, state or local laws or regulations;
- Activities that violate legal protections provided by patents, copyrights, trademarks, and Intellectual property rights;
- Chain letters;
- Recreational games;
- Unauthorized disclosure of CARNIVAL GROUP Business Critical Information;
- Unauthorized access, or attempted access or entry, to any other network or computer.

## Portable Computing Device Use

**[38]** Where the device supports it, the power-on, or security password, must be enabled. Note: Some portable computing devices limit password strength. If a password conforming to the requirements of the **Password and PIN Security Policy** cannot be used, then the strongest password permitted by the device should be used. Note: for a Windows 2000 device, the security password is the network access password that is also used for login to the device when it is not network connected.

**[39]** Automatic login scripts, which would allow an unauthorized party access to an account without requiring a password, are prohibited.

**[40]** When not in use, authentication tokens (e.g. Secure ID cards, smart cards, CARNIVAL GROUP Tokens) should be kept separate from the portable computing device and its case.

**[41]** Portable computing devices must not be left unattended when remotely connected to CARNIVAL GROUP, even if physically secured.

**[42]** Portable computing devices should be protected in accordance with the value of the information contained in the device, and not be left unattended.

**[43]** Business Critical Information must be protected at all times.

**[43.1]** Business Critical Information can be stored on removable media (e.g., Zip disks, tapes, flash memory cards, CDs, USB memory devices) and the Removable media physically protected (e.g., locked in a safe, or kept with the individual). These Medias should be returned to IT Department/immediate supervisor in case of resignation or termination of service.

**[43.2]** Handheld PCs, Palm-size PCs, Smart Telephones, PDAs, etc. that can be physically carried by the user must be protected as one would protect a wallet or similar container that holds ones identity (e.g., driver's license, credit cards, etc.).

**[43.3]** Handheld PCs, Palm-size PCs, Smart Telephones, PDAs, etc shall not be used to store or transmit Business Critical Information (including e-mails and attachments to emails) unless these devices are in compliance with all of the Policies.

**[43.3.1]** If the device is synchronized with a personal computer, the Business Critical Information transferred should be appropriately protected on the PC in accordance with other CARNIVAL GROUP policies.

**[44]** Up-to-date, anti-virus software (including virus definitions) must be installed and automatic scanning enabled, when such software is available. All externally obtained media or files should be scanned before any files are opened.

**[45]** Backup of any data stored on portable-computing devices is the responsibility of the user.

**[46]** Business Critical Information must not be accessed on airplanes or in public places unless the users are absolutely certain that only they can read the information on the portable computing devices screen.

**[47]** Loss of a portable computer device or the loss of removable media that contains Business Critical Information must be reported to the individual's manager, and IT department as soon as possible, but not later than 24 hours after detection of the loss.

**[48]** When good judgment has not been exercised in safeguarding a portable-computing device, the individual may be subject to disciplinary action and may be held responsible for the replacement cost if the device is lost or stolen.

## Encryption

**[49]** Only CARNIVAL GROUP -approved cryptographic algorithms and supporting processes may be used to protect Business Critical Information.

**[50]** The preferred device for CARNIVAL GROUP Subscribers is a hardware token with pass phrase access to the securely stored private keys and to execute cryptographic functions. .

**[51]** Data in the CARNIVAL GROUP Enterprise Directory shall adhere to the following requirements:

**[51.1]** Data must come from an Authoritative Source.

**[51.2]** The Authoritative Source is responsible for the accuracy and timeliness of Data provided to the Enterprise Directory.

**[51.3]** No data from an Authoritative Source shall be entered or modified without a signed Provider Agreement:

**[51.4]** Only one Authoritative Source for any single data item is permitted.

**[51.5]** Only the Authoritative Source shall make changes to the Directory data that it has entered.

**[52]** Relying Party acceptance of a digital signature generated by a CARNIVAL GROUP PKI Subscriber shall be controlled by CARNIVAL GROUP and its Operating Companies (if the relying party is a CARNIVAL GROUP employee), or through contracts.

**Exception:** CARNIVAL GROUP may decide not to use encryption software as per its business requirement, based on the recommendation from IT head and approval by Operations head.

## Modems

**[53]** No desktop computer, portable computer, or portable computing device shall be connected simultaneously to more than one network (a B2B VPN where the device is connected to a partners network which is itself connected to CARNIVAL GROUP, is considered to be "one network").

## Non CARNIVAL GROUP Computing Devices

**[54]** CARNIVAL GROUP employees or Business Partner employees personally-owned computing Devices are prohibited from connecting to and accessing CARNIVAL GROUP, either directly or via remote access until approved by user department head &IT head.

## Reporting

**[55]** All persons with access to CARNIVAL GROUP information assets must report any known or suspected violation of the CARNIVAL GROUP Policies to their local management and their local Information Security Officer. If the violation involves a security incident, this will be done in accordance with the reporting and escalation hierarchy specified in other CARNIVAL GROUP policies.

**[56]** Users must notify the local help desk whenever a computer virus is suspected or detected.

**[57]** Loss of a portable computer device or the loss of removable media that contains Business Critical Information must be reported to the individual's manager, and IT department as soon as possible, but not later than 24 hours after detection of the loss.

## User Installed Software

**[58]** Users and administrators are accountable for all software that is used on machines under their control.

**[58.1]** Users are prohibited from installing unauthorized software on CARNIVAL GROUP computers.

**[58.2]** Users are strongly discouraged from using software downloaded from the Internet, or other non-CARNIVAL GROUP. However, if such software is required for business purposes, users are responsible for obtaining management approval of the business need and IT heads approval for security risk.

**[58.2.1]** Users shall ensure that virus scanning is completed on all software obtained in this manner.

**[58.2.2]** If automatic scanning of files is not enabled or temporarily disabled, or no anti-virus software is installed on a device, the users and administrators must manually scan any portable storage devices (floppies, CDs, etc.), downloaded executable or downloaded compressed files (e.g., ZIP files) on another system prior to installation.

## Access Control Gateway Security Policy

**Objective: All Information Assets, interconnections between any external network and CARNIVAL GROUP must be continuously protected by an access control system using various protection & control technologies.**

## Minimum Implementation Standards:

### General

**[1]** All external accesses to CARNIVAL GROUP or to any CARNIVAL GROUP computing device connected to a non-CARNIVAL GROUP (including, but not limited to the Internet) must pass through an access control system (such as a firewall) where all traffic between CARNIVAL GROUP and external networks can be continuously controlled, monitored and examined for any access violations. Bypassing gateway security mechanisms is prohibited.

### Access Control

**[1]** CARNIVAL GROUP must be protected by one or more authorized firewalls managed by CARNIVAL GROUP that define and enforce rules over information and users crossing internally to external systems, or from external systems to internal resources, including CARNIVAL GROUP information services provided via a service segment [a.k.a. Demilitarized Zone (DMZ)].

**[2]** All inbound access to CARNIVAL GROUP must have an approved business purpose and associated risk assessment.

**[3]** Remote users may not access CARNIVAL GROUP systems through unauthorized modems placed behind a CARNIVAL GROUP firewall.

**[4]** All CARNIVAL GROUP firewall servers must have inbound and outbound rules to allow or deny connections. All access not explicitly allowed must be denied.

**[5]** All CARNIVAL GROUP firewall servers or appliances must be equipped with approved dynamic intrusion detection and alerting mechanisms.

**[6]** Intrusion thresholds must be set at levels at which automated alarms and/or preventive actions are initiated.

**[7]** All CARNIVAL GROUP firewall server or appliance configurations must be kept as "user-friendly" as possible to avoid errors in the configuration that might compromise the effectiveness of the protection provided. Configurations must be reviewed by CARNIVAL GROUP IT at least quarterly.

**[8]** Firewall rules to prevent source routing and spoofing attacks must be included in the configuration.

**[9]** All changes to the firewall require a risk assessment and must be approved prior to implementation by the CARNIVAL GROUP IT Head.

**[10]** If an CARNIVAL GROUP firewall requires an operating system, a secured version of the operating system, with all patches installed in accordance with **Information System Administration and Management Security Policy** must be a part of the firewall. These patches must be installed no later than two weeks after their availability from the vendor. (Note: There should be an identified need for the patch in the CARNIVAL GROUP computing environment and the patch should first be tested offline before being introduced into production systems to ensure it will not cause instability or malfunction.)

## Logging and Auditing

**[13]** All CARNIVAL GROUP firewall servers or appliances must contain mechanisms for logging traffic and suspicious activity.

**[14]** All CARNIVAL GROUP firewall servers or appliances must contain mechanisms for log reduction to ensure that logs are readable and understandable.

**[15]** Operating Companies must implement a local process covering the log period for reviewing logs, and this process must be documented. The log review period must be commensurate with the assessed risk for the resource(s) being monitored and adhere to the following:

**[15.1]** Logs for Internet and Business Partner-facing servers or appliances shall be reviewed weekly.

**[15.2]** Logs for all other systems shall be reviewed no less frequently than once a month.

**[15.3]** Exception: For whatever level of review the data owner has decided, this Requirement for log reviews can be met using host-based intrusion detection in accordance with other CARNIVAL GROUP policies.

**[16]** Knowledge of CARNIVAL GROUP firewall passwords must be restricted to the minimum number of people necessary and they shall be securely maintained.

**[17]** All CARNIVAL GROUP firewall server consoles shall not display the last user to log in.

**[18]** All CARNIVAL GROUP firewall servers or appliances shall be logged off or logically locked when unattended.

## Internal Firewalls

**[19]** The use of internal firewalls as an internal gateway security function for providing increased or additional security, and access control to highly sensitive areas or applications, is permissible and encouraged.

**[20]** Internal firewalls should be configured and managed in accordance with this policy and be no less stringent in the specification of access control rules than Internet facing firewalls.

## Additional Security

**[21]** In addition to the use of firewalls, the following measures shall be applied, where appropriate, to enhance security:

**[21.1]** All CARNIVAL GROUP firewall servers or appliances shall utilize a properly sized Uninterruptible Power Supply (UPS) power system to maximize service availability and minimize the risk of data loss.

**[21.2]** All CARNIVAL GROUP firewall servers or appliances shall be operated in environments that are within the hardware manufacturer’s recommended environmental ranges for equipment operation.

**[21.3]** Physical access to CARNIVAL GROUP firewall servers or appliances and associated equipment must be restricted only to those individuals who require access to perform their duties.

**[21.4]** All CARNIVAL GROUP firewall servers or appliances shall be CDROM-boot disabled and DVD-boot disabled if they have any of these features.

**[21.5]** All CARNIVAL GROUP firewall servers or appliances shall have a Disaster Recovery Plan (DRP) in case of hardware or software failure or attack.

## Wireless LAN

**[21.1]** All CARNIVAL GROUP WLAN access point should be on separate subnets or separated from company network by a firewall.

**[21.2]** Default values and configuration must be changed before deployment as per CARNIVAL GROUP Policies.

**[21.3]** **WPA** or higher encryption must be enabled to ensure the strong encryption of data between WAP and client machines.

**[21.4]** All CARNIVAL GROUP **WAP** (Wireless Access Points) devices must be authenticated with company name zone-specific identifiers where possible. Access points must not broadcast SSID.

## Policy on Physical Security of Information Assets

**Objective: Physical access to facilities and equipment that contain or process Business Critical Information must be adequately controlled.**

## Minimum Implementation Standards:

### [1] Access Control

**[1.1]** The degree of access control must be commensurate with the value of the Business Critical Information available at the location, (building, office, etc.).

**[1.2]** Everyone (employees, visitors, resident contractors, etc.) should wear identification badges.

**[1.3]** Visitor and contractor registries must be maintained.

**[1.4]** Escorts for visitors must be provided whenever Business Critical Information is readily accessible within the facility.

**[1.5]** Escorts for visitors must be revoked immediately upon resignation or termination of employees and whenever contracts or contractor work are completed.

**[1.6]** Unattended areas that contain Business Critical Information must be locked to Control unauthorized entry.

**[1.7]** Appropriate exit controls should be in place to control unauthorized removal of information and equipment.

**[1.8]** Data Centers must have a unique register for all visitors. This registry is in addition to the register of the location (campus, building, office, etc.).

**[1.9]** All data centers, equipment rooms and telecommunication closets must be locked and/or have strong access controls.

**[1.10]** Employees, supplier-partners and visitors should be advised by posted signage at entrance points, visitors log headers and through inclusion in employee and supplier nondisclosure agreements, that the use of photographic recording or transmission technology is prohibited on company property absent written authorization from a sponsoring Manager.

## [2] Equipment Security

**[2.1]** Only authorized maintenance personnel may perform installation and repair.

**[2.2]** A record of equipment failures and maintenance actions should be maintained.

**[2.3]** Equipment that is power dependent must be protected from power failures, surges and other electrical anomalies.

**[2.4]** Uninterruptible Power Supplies (UPS) must be used for equipment supporting high availability business critical operations.

**[2.5]** Power, telecommunication, and network cabling must be adequately protected from unauthorized access and intentional or unintentional damage.

**[2.6]** Devices used to process or store Business Critical Information (e.g., desktops, laptops, printers, fax machines, etc.) must be adequately protected from theft and loss.

**[2.7]** Any loss or damage to computing devices must be reported and a Damage Assessment Report filed in accordance with **Portable Computing Device Security Policy.**

**[2.8]** All equipment that contains or could have contained Business Critical Information must be checked to ensure that all such information has been removed prior to disposal.

**[2.8.1]** Information stored on magnetic media must be removed using an approved degaussing/overwriting process before discarding.

**[2.8.2]** Paper or film-based media must be destroyed using approved destruction devices/processes, e.g. cross-shredding or alkaline, acid or solvent based process, before discarding.

## Portable Computing Device Security Policy

**Objective: All portable computing devices used to process and store Business Critical Information must be controlled and physically protected and must be afforded security appropriate to their contents.**

## Minimum Implementation Standards:

### Access

**[1]** Where the device supports it, the power-on, or security password, must be enabled.

**Note**: Some portable computing devices limit password strength. If a password conforming to the requirements of the **Password and PIN Security Policy** cannot be used, then the strongest password permitted by the device should be used.

**Note:** For a Windows 2000 device, the security password is the network access password that is also used for login to the device when it is not network connected.

**[2]** Automatic login scripts, which would allow an unauthorized party access to an Account without requiring a password, are prohibited.

**[3]** When not in use, authentication tokens (e.g. SecurID cards, smart cards, JJEDS Tokens) should be kept separate from the portable computing device and its case.

**[4]** Portable computing devices must not be left unattended when remotely connected to CARNIVAL GROUP, even if physically secured.

**[5]** Portable computing devices should be protected in accordance with the value of the information contained in the device, and not be left unattended.

### Protection

**[6]** Business Critical Information must be protected at all times.

**[6.1]** Business Critical Information can be stored on removable media (e.g., tapes, flash memory cards, CDs, USB memory devices) and the removable media shall be physically protected (e.g., locked in a safe, or kept with the individual).

**[6.2]** Handheld PCs, Palm-size PCs, Smart Telephones, PDAs, etc. that can be physically carried by the user must be protected as one would protect a wallet or similar container that holds ones identity (e.g., driver's license, credit cards, etc.).

**[6.3]** Handheld PCs, Palm-size PCs, Smart Telephones, PDAs, etc. shall not be used to store or transmit Business Critical Information (including e-mails and attachments to emails) unless these devices are in compliance with all of the CARNIVAL GROUP Policies.

**[6.3.1]** If the device is synchronized with a personal computer, the Business Critical Information transferred should be appropriately protected on the PC in accordance with the CARNIVAL GROUP Policies.

**[7]** Up-to-date, anti-virus software (including virus definitions) must be installed and automatic scanning enabled, when such software is available. All externally obtained media or files should be scanned before any files are opened.

**[8]** Backup of any data stored on a portable computing device is the responsibility of the user.

**[9]** Business Critical Information must not be accessed on airplanes or in public places, unless the users are absolutely certain that only they can read the information on the portable computing devices screen.

## Reporting Losses

**[10]** Loss of a portable computer device or the loss of removable media that contains Business Critical Information must be reported to the individual's manager, and IT department as soon as possible, but not later than 24 hours after detection of the loss.

**[11]** The owner of a computing device or removable media that is reported lost, or whose data are suspected of being compromised, is required to file a Damage Assessment Report with the IT department as soon as possible, but not later than 24 hours after the detection of the loss.

**[11.1]** The Damage Assessment Report should specify the nature of the compromised data, (e.g., Business Critical Information) and those parties that might be impacted by the loss (e.g., Finance, Marketing, Public Relations, etc.). The Damage Assessment Report should also specify whether any mechanisms were in place at the time of the loss to protect the data, such as encryption or password protection.

**[12]** When good judgment has not been exercised in safeguarding a portable computing device, the individual may be subject to disciplinary action and be held responsible for the replacement cost if the device is lost or stolen.

## System and Application Lifecycle Security Policy

**Objective: All systems and applications that process or store CARNIVAL GROUP Business Critical Information shall address information security requirements during all phases of the development cycle.**

## Scope:

**This policy applies to Systems and Applications regardless of where or by whom they are developed or deployed.**

## Minimum Implementation Standards:

## Security Requirements Analysis and Specifications

**[1]** The Information Owner and the valuation of the information stored, processed and communicated by the system (refer to **Information Valuation and Protection Policy)** shall be determined prior to the development of security requirements and specifications.

**[2]** A comprehensive security requirements analysis and specification shall be performed for all new systems and applications or significant upgrades to existing systems. This analysis shall demonstrate that the System or Application meets the applicable **Information Asset Protection Policies**. This security analysis also applies to "pilot" programs and to "new technology" investigations. The analysis shall identify any valid requirements in security and security related areas such as:

- Confidentiality
- Authentication
- Authorization
- Administration
- Malicious software control
- Event logging
- Event auditing
- Scalability
- Non-repudiation
- Access control
- Integrity
- Configuration
- Intrusion detection
- Fault tolerance
- Capacity
- Public key cryptography/ digital certificates

**[3]** System/Application security requirements and specifications must be compliant with standards for technologies and system configuration, CARNIVAL GROUP Standards and CARNIVAL GROUP Design documents, where applicable.

**[4]** **System**/Application security requirements and specifications must require interoperability with all information sources and services with which it must interface.

**[5]** System/Application security requirements and specifications must ensure integration with existing security services, where applicable and appropriate.

**[6]** **Additional** security assessments must be performed to address any changes to the System/Application.

## Security Verification

**[7]** All new Systems/Applications must be tested in a separate environment for stability and to identify any unanticipated interactions with existing systems before they are introduced into the production/operations environment.

**[8]** All new Systems/Applications must be tested for security integrity and functional verification, in accordance with requirements and specifications, prior to general availability.

**[9]** The CARNIVAL GROUP IT Head is responsible for ensuring that a process is in place to approve all new System Application installations connected to or associated with CARNIVAL GROUP.

**[10]** If the new System/Application will connect to CARNIVAL GROUP, then CARNIVAL GROUP must also approve the System to indicate that there will not be a negative impact to CARNIVAL GROUP security.

**[11]** IT Head, in consultation with Operations head within the company must make final approval of System/Application security.

## Development and Testing

**[12]** Production/Operations Systems/Applications will not be used for development or testing activities.

**[13]** All security features and functions will be operated during formal acceptance and operational tests.

**[14]** Prior to making a new system or an upgrade to an existing system available for general use, testing will be done to ensure the new System/Application does not adversely affect any existing systems.

**[15]** New (or major upgrades to existing) Systems/Applications will be approved for use at the Company by the IT head within the company prior to operating the System in the production/operational environment.

**[15.1]** If required third party can be hired for in-depth evaluation and Reports.

**[15.2]** For new business requirements the system evaluation, testing, will be done as per **System & Application Acquisition policy.**

## Operation

**[16]** Production/Operations Systems and Applications will be operated and managed in accordance with the CARNIVAL GROUP Information Asset Protection Policies, including, but not limited to:

- **Access Control Policy**
- **Anti-Virus and Malicious Software Protection Policy**
- **Password and PIN Security Policy**
- **User Responsibility Policy**
- **Business Continuity and Disaster Recovery Policy**
- **Information System Administration and Management Security Policy**

## Continuity of Service

**[17]** A fallback plan must be devised for recovery of existing services in the event that introduction of a new system causes service degradation or interruption.

**[18]** A cutover plan must be written prior to rollout of a new system to ensure continuity of service.

## Business Continuity and Disaster Recovery Policy

**Objective: All CARNIVAL GROUP Companies must institute and practice an Information Systems Continuity of Business and Disaster Recovery Plan that will prevent catastrophic data loss and ensure timely restoration of networking and computing services in the event of system failure or destruction.**

## Minimum Implementation Standards:

## General

This policy presents minimum requirements for the contents of an Information Systems Continuity of Business and Disaster Recovery Plan. It focuses on the mission critical information assets. The policy does not cover the related areas of contingency planning, crisis management and emergency management. Therefore, expansion of this policy, or its incorporation into a broader business continuity and disaster recovery plan, as appropriate, is strongly encouraged. The recovery objectives are to:

- Ensure minimal impact on service (meet service continuity requirements);
- Minimize impact on revenue, assets, and CARNIVAL GROUP's reputation; • Ensure availability of mission critical functions after an incident; and
- Meet regulatory, fiduciary, and CARNIVAL GROUP Ethics & Credo requirements.

**1.** Plans should enable the continuity of mission critical functions in case of an emergency by evaluating the need to maintain the systems that support those functions at alternate sites, and by implementing them at alternative sites where that makes sense. Upon declaration of an information systems disaster by a company's Chief Executive Officer (or equivalent position), the plan will be implemented. If implementation involves deployment to alternate sites, operations may continue from those facilities for a period of time as appropriate, or as contracted.

**[1.1]** To meet appropriate restoration timelines, computing capacity needs to be readily available and backup data must be as close to the point of incident as is deemed reasonable.

**[1.2]** Successful continuity of business and disaster recovery relies upon having a regularly tested plan for all recovery processes. Care must be exercised so that this testing does not interfere and/or disrupt damage or otherwise alter the normal day-today operations of the business.

## Roles and Responsibilities

**[2]** Implementation of the Continuity of Business and Disaster Recovery Plan will be accomplished using an organized approach that clearly identifies a line of authority. The Company Chief Information Officer/ IT Head must designate, in writing, a Business Continuity/Disaster Recovery Coordinator who, in close coordination with the company's Chief Executive Officer (CEO), will be responsible for the following for all Company facilities:

- Planning development, maintenance, testing, and mitigation, response,
- Restoration, and resumption activities;
- Implementing the Business Continuity/Disaster Recovery Plan; and
- Executing the Plan when the Operations Head declares an information systems Disaster.

**[3]** The duties defined and assigned in this policy will be reviewed and/or revised upon events such as organizational realignments, acquisitions or divestitures, or the departure of any personnel with key disaster recovery/business continuity responsibilities.

## Prioritization

**[4]** Determining the criticality of systems that support mission critical functions and the impact of loss of those systems to the Company is not a static activity. The Company must understand the dynamic nature of their information systems environment and the relationship of new systems and applications in that environment.

**[4.1]** Each Company will support the Information Systems Continuity of Business and Disaster Recovery Plan by performing a business impact analysis, under the direction of the Business Continuity/Disaster Recovery Coordinator to:

Identify mission critical systems and applications;

Determine the criticality of those systems to the Company; and identify the impact to the Company if those systems and applications are disrupted over a period of time.

**[4.2]** Each Company's business impact analysis will include a comprehensive Risk assessment That identifies:

- Business impacts;
- Threats, hazards, and vulnerabilities;
- Human impacts;
- Communications impacts;
- Facility concerns; and
- Security concerns

**[4.3]** Items to be considered as part of the business impact analysis include building, electrical, mechanical, security, and fire safety specifications and requirements, facility recovery alternatives, system and application criticality criteria, system, application, and process interdependencies, vital business processes, vital systems, and vital records, and backup processing/network alternatives. Also, a recommended recovery strategy based upon an optimum cost/benefit to the Company will be formulated.

## Prevention

**[5]** Each Company will need to perform a risk analysis. The risk analysis process must consider and address all relevant threats to the mission critical information systems for each facility. The results of the risk analysis process must be combined with the results of the prioritization effort to determine the controls that need to be put into place to deter, mitigate, or reduce the threats to the Company. In the information systems area, the criticality of the application systems and the recovery time objectives for the systems that are run at each facility will determine the types of controls that will need to be put into place. Examples of controls that could be used to deter, mitigate, or reduce the effect of threats to information systems include:

- Redundant or fault-tolerant hardware
- Automatic fail-over hardware
- Uninterruptible Power Supplies (UPS)
- Hot or cold spares
- Service provider Quality of Service (QoS) agreements
- Fire prevention, detection, and remediation systems
- Alternate Processing Sites (Hot, Warm, Cold)
- Alternate Processes (e.g., Fax v. E-Mail, etc.)

**[5.1]** The cause and effect relationship of threats and risks is evaluated against The probability of the threat actually occurring. The probability of the threat occurring is how vulnerable the organization is to the threat. The risk analysis will attempt to prevent the threat from occurring, and if that is not possible, then it will mitigate the impact if the risk occurs.

**[5.2]** Quantitative and Qualitative approaches should be employed when evaluating the results of a risk analysis. A quantitative statement of risk assigns an objective value (such as money) to the particular threat. In other words, how much will it cost the Company if this threat occurs? The qualitative statement of risk is used for threats that are difficult to assign hard monitory values – the special qualities or effects of the threat make it what it is.

**[5.3]** After these determinations have been made, an analysis will be done using Business needs and return-on-investment considerations to determine if it will be a sound business practice to develop controls to address the threat. Once that analysis has been completed and it is determined that the threat must be addressed, controls will be developed and put into place that will deter the threat from occurring, mitigate the impact of the threat, or reduce the effect of the threat if it occurs.

## Documentation

**[6]** One of the crucial resources for reconstructing a failed system is complete, accurate, and up-to date documentation. The documentation of the Company's business continuity processes and procedures into a comprehensive Continuity of Business and Disaster Recovery Plan, in advance, is critical to ensure the continuity of the mission critical functions of the Company. It is imperative that all information related to system design, configuration, and administration be continuously maintained and available to recover. The **Information System Administration and Management Security Policy** contains specific documentation requirements.

**[7]** The Continuity of Business and Disaster Recovery Plan is developed at the Company level. All of the Continuity of Business and Disaster Recovery Plans developed at the facility level will coordinate with the Company level Continuity of Business and Disaster Recovery Plan. Each Plan will include the following information:

Recovery requirements for each mission critical system, including priority order of recovery and required timeframes;

Contact and notification information, including notification procedures to those key operating personnel responsible for the identified systems;

Computer recovery configuration requirements; and

Off-site storage strategy for all data and vital documents.

## Data Backup

**[8]** The Information Systems Continuity of Business and Disaster Recovery Plan documents the requirements and processes for the restoration and verification of the recovered operating environment, network, data, and mission critical business functions.

**[8.1]** Accurate, complete, and current documentation of the operating environment is required for all mission critical business functions within the Company. Backup documentation and files will be maintained that contain information detailing the technical configurations for the operating environment, infrastructure, network, machine configurations, and across platform connectivity requirements. Documented aspects of the environment will be included as appendices within the Information Systems Continuity of Business and Disaster Recovery Plan.

**[8.2]** Changes to the Company's operating environment will be captured during the change Control Review process and updates will be made to the Information Systems Continuity of Business and Disaster Recovery Plan to reflect the approved environment changes.

## Safety

**[9]** The Continuity of Business and Disaster Recovery Coordinator will establish processes and procedures to help ensure the safety of all personnel employed by, under the direct supervision of, or subcontracted by the Company. These must be closely coordinated with CARNIVAL GROUP Crisis Management, Company Security, local, state and federal agencies, as Appropriate. Safety aspects to be considered, and included in the Plan where appropriate:

- **i** Building evacuation and re-entry rules and procedures
- **ii** Evacuation of handicapped personnel procedures
- **iii** Contact information with local, state, or federal fire, police, and emergency Services
- **iv** Employee illness or injury procedures
- **v** Evacuation procedures
- **vi** Procedures to respond to bomb threats
- **vii** Explosions
- **viii** Casualties
- **ix** Physical Assaults
- **x** Chemical Spills
- **xi** Natural disasters such as floods, earthquakes, storms Biological threats and contamination

## Testing

**[10]** Testing will be used to practice procedures before a disaster to ensure that the written Procedures are actionable and effective, and to train personnel in emergency procedures.

**[10.1]** The actual operations testing of the Continuity of Business and Disaster Recovery Plan will be conducted in stages. Best practices recommend that operations testing begin on a limited scale and build to a full test of the Continuity of Business and Disaster Recovery Plan.

**[10.2]** The testing schedule for the Continuity of Business and Disaster Recovery Plan will be established for as far into the future as possible. The full Continuity of Business and Disaster Recovery Plan must be tested at least once per calendar year.

## Updating

**[11]** A Continuity of Business and Disaster Recovery Plan cannot be a static document. Information system environments constantly change and the plan must reflect operating Infrastructure, processing and environment changes.

**[11.1]** Information Systems Continuity of Business and Disaster Recovery Plans will be updated whenever system changes are made that would cause them to become invalid or ineffective. System changes include changes to communication infrastructure, technical infrastructure and/or applications supporting critical business functions. As a part of the standard System Development Life Cycle and Change Control Review Process, impacts to the Information Systems Continuity of Business and Disaster Recovery Plans will be reviewed and necessary changes incorporated into the affected areas.

**[11.2]** The Business Continuity/Disaster Recovery Coordinator will review Information Systems Continuity of Business and Disaster Recovery Plans annually and prior to any planned test event.

## Data Backup Policy

**Objective: The purpose of the systems backup is to provide a means to: (1) restore the integrity of the computer systems in the event of a hardware/software failure or physical disaster, and (2) provide a measure of protection against human error or the inadvertent deletion of important files.**

**Scope** **This policy applies to all equipment and data owned and operated by the organization.**

**[1.0] Timing** Full backups are performed nightly on the first attempt irrespective of the weekly days and then an incremental backup being carried out once in a day for the rest of the week days. If for maintenance reasons, backups are not performed on any day, they shall be done immediately on the next day.

**[2.0] Responsibility** The IT department manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

**[3.0] Testing** the ability to restore data from backups shall be tested at least once per month.

**[4.0] Data Backed Up** Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. User Data on Network Drives

**[5.0] Archives**

On the basis of the advance request from the HOD (prior to receiving the Full and Final Form (FnF) generally on last working day) archives of the users data and emails can be made on request and handed over to the HOD.

**[6.0] Restoration**

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

**[7.0] Storage Locations** In case of any Offline tapes/removable storage used for nightly backup shall be Stored in an adjacent building in a fireproof safe. Weekly backup will be transferred to Mumbai office every Saturday and Sunday and overwritten the following week.

Exceptions to the standard procedure are permitted when justified. All exceptions must be fully documented. The standard procedure for systems backup is as follows:

1. A full systems backup will be performed weekly. Weekly backups will be saved for a full month.
2. The last weekly backup of the month will be saved as a monthly backup. The other weekly backup media will be recycled for other uses or destroyed.
3. Monthly backups will be saved for one year, at which time the media will be recycled or destroyed.
4. Incremental backups will be performed daily. Incremental backups will be retained for two weeks, at which time the media will be recycled or destroyed.
5. All backups will be stored in a secure, off-site location. Proper environment controls, temperature, humidity and fire protection, shall be maintained at the storage location.
6. All backup media that is not re-usable shall be thoroughly destroyed in an approved manner. Backup media that is used for other purposes shall be thoroughly erased.
7. Periodic tests of the backups will be performed to determine if files can be restored.

## Mobile computing devices policy

**Objective: To develop and practice an enterprise wide policy which describes the rules covering use of mobile computing devices that can be attached to CARNIVAL GROUPs, or containing CARNIVAL GROUP Information. This includes, but is not restricted to, Personal Digital Assistants (PDA's), tablets, Smart phones, Mobile phones and Blackberries.**

### Scope

All CARNIVAL GROUP supplied mobile devices and their contents remain the property of CARNIVAL GROUP and are subject to regular audit and monitoring. These devices should only be connected to a laptop or desktop that has been approved for use at the CARNIVAL GROUP. Users must be aware that the device contains CARNIVAL GROUP data, and take appropriate action to protect the device from being lost or stolen.

Only company provided devices which have been built to CARNIVAL GROUP published standards and/or from approved suppliers, should be attached to the CARNIVAL GROUP data network wired or wireless either directly or through a CARNIVAL GROUP (owned or leased) PC or laptop. This should ensure that appropriate security controls have been built into the implementation.

Once received, the user is not authorized to change any security device settings without reference to the IT desk, as they may affect the security of the device, or stop it functioning with the supplied service. Phone software updates can be installed on phone by IT team after the approval of IT head.

In certain business situations there is a need to attach non-CARNIVAL GROUP owned devices. Only devices that do not directly attach to the CARNIVAL GROUP data network can be authorized (i.e. only devices that connect to a CARNIVAL GROUP desktop or laptop PC, via infrared, Bluetooth or USB – this is restricted to a few PDA's and smart phones). Devices eligible for these dispensations are limited to smart phones or PDA's. These devices must have their security settings (passwords etc.) configured as per the requirements detailed in this document.

If a CARNIVAL GROUP owned device is lost or stolen, then the Service Desk should be contacted on 022 67886100/108/102 as a matter of urgency, so that device configuration can be deleted from the server. User should ensure that he regularly back-up CARNIVAL GROUP data on the device to CARNIVAL GROUP equipment to protect the data from damage or loss.

Where there are security settings held in the device (such as a PDA), ensure you back the device up to a removable memory device to ensure that it can easily be reconfigured.

If the information you carry has been classified as CARNIVAL GROUP Confidential, then this information should not be carried on mobile devices unless it is encrypted (where this facility is available on the device, where it is not, the user must consider carefully before allowing it to be stored on the device). Blackberries will potentially receive confidential information via e-mail; this is recognized and allowed until an encrypted solution is available.

### [2.0] Approved Devices & their Security Requirement

Please ensure that your devices are configured as below:

1. **Mobile devices**- alphanumeric password locked whilst not in use.

2. **MP3 Players (e.g. MP3 enabled phones, I-phone, and iPods)** - Users should not connect personal MP3 players to official laptops and stores personal music. Where personal devices are also storing CARNIVAL GROUP content, permission must have been gained from the department head. Users MUST acquaint themselves of the legal situation for any personal content stored.

### [2.0] Prohibition.

**[2.1]** No changes to the security settings or configuration of any approved device can be made without prior authorization from IT.

**[2.2]** Never attempt to use an unapproved device, via any method of communication, with any IT equipment that belongs to the CARNIVAL GROUP.

**[2.3]** Personal mobile phones with cameras and personal digital cameras are permitted in the office but must not be used to collect and store data that belongs to the CARNIVAL GROUP.

**[2.4]** CARNIVAL GROUP IT team reserves the right to remote swipe a Mobile device based on written approval from the HOD.

### [3.0] Specific points on the use of Camera Phones/tablets.

a) Cameras enabled phones should primarily be used for taking business related pictures. However, some limited personal use is allowed, but storage must not interfere with CARNIVAL GROUP Business use.

b) Inappropriate content prohibition applies to mobile phones as it does other forms of communication.

c) Information should be downloaded to a secure device (CARNIVAL GROUP Laptop for example) and removed from the phone at the user’s earliest opportunity.

d) Privacy, only take pictures of individuals with their permission to do so, or follow current policy where this is impractical.

**[3.1] Specific points on the use of Bluetooth enabled devices.**

a) Bluetooth must only be used for accessing passive devices – such as hands free Kits.

b) Bluetooth cannot be used to communicate with a device directly connected to the CARNIVAL GROUP data network (unless through a CARNIVAL GROUP owned or leased PC).

c) Bluetooth connections must be accepted from other devices with care. Ensure the recipient is known and agree connection security criteria in advance.

d) Never run an CARNIVAL GROUP device in broadcast mode, various viruses and other schemes are prevalent whilst in this mode.

**[3.2] Specific points on the use of Infrared enabled devices.**

a) Infrared must only be used for accessing passive devices; no sync should be performed using the interface (unless through a CARNIVAL GROUP owned or leased PC).

b) Infrared cannot be used to communicate with other devices, and should be turned off.

c) No CARNIVAL GROUP data can be sent to other devices (including CARNIVAL GROUP owned ones) using the Infrared protocol.

**[3.3] Specific points on the use of non-CARNIVAL GROUP owned devices.**

a) Only devices provided to level one and above are currently supported. If the device requires special software to be incorporated onto the desktop, this is not allowed.

b) If the user wants to any other device then the one provided by the company then the device should support encrypted communication and an antivirus must be installed on the same.

c) The permission to attach non-CARNIVAL GROUP devices is prior arranged by job function and division through the IT Head.

## Cloud computing policy

.

**Objective: To assist CARNIVAL GROUP in the use of cloud computing services to support the processing, sharing, storage and management of data**

**Scope.** **This policy provides basic guideline on usage of Cloud technology in CARNIVAL GROUP Business processes.**

### A. Identification of Applications & Services

a) Assessment of applications should be conducted to identify applications that can be hosted/ used in a cloud computing environment

b) Assessment of current infrastructure vis-à-vis desired infrastructure should be conducted to identify the feasibility of acquiring cloud computing services

c) Criticality of the application should be assessed based on which the type of cloud should be selected. For e.g. a private or internal cloud is used for applications with very sensitive/ secret information

d) The current maintenance cost against the cost of cloud computing services should be considered before making any decisions

e) The Risk (application, architecture, data location/retrieval, legal & regulatory, privacy, security, etc.) associated with hosting the application in a cloud computing environment should be taken into consideration

f) The flexibility provided with the use of cloud computing against the rigid internal network should be considered

g) Security and privacy control should be identified, documented and implemented while configuring applications on cloud environment

h) Scalability, efficiency and availability requirements should be assessed for the applications to be hosted on a cloud computing environment

i) All communication and remote access should be encrypted and monitored as per the communication policy

j) The cloud computing providers and their service offerings should meet requirements of Protective Security Policy Framework (PSPF) and the Privacy Act 1988

k) CARNIVAL GROUP should maintain assurance that the security of cloud computing provider is in accordance with the PSPF by performing periodic checks

l) CARNIVAL GROUP should ensure that the cloud computing service provider has business continuity in place for cloud and related infrastructure

m) Security controls should be implemented according to threat, and vulnerability risk assessment of the information

n) Users should be provided access to cloud computing systems as per the access management policy

o) Encryption techniques should be used for data and communications

p) Software as a Service (SaaS) model should be implemented for managing cloud computing architecture

## Contractual agreement with cloud service providers

1. Collection: The cloud computing service provider should be restricted from collecting and storing confidential information
2. Use and disclosure: Restrict the cloud computing provider from using or disclosing confidential data
3. Service levels for availability and performance should be mentioned in the agreement
4. Clauses for security, at the cloud, the supporting infrastructure and communication channels should be included in the agreement
5. Confidentiality of information and privacy concerns should be addressed in the agreement
6. The location (physical and logical) of the data storage area should be included in the agreement so as to identify where the confidential data resides
7. CARNIVAL GROUP should ensure that the cloud-computing infrastructure resides in an area governed by legal laws and regulations.
8. CARNIVAL GROUP should ensure that the cloud computing provider adheres to standards for interoperability, data portability and use of commercial off the shelf products
9. Clauses for penalty and law suit in case the cloud computing provider does not adhere to availability, security and privacy requirements should be included in the agreement

# RISK ASSESMENT

## Introduction

A Risk Assessment is a careful examination of threats, vulnerabilities, and the probability of threat exploiting a vulnerability which may harm, cause loss or damage to company's Information and Information Systems.

A Risk Assessment involves:

- Identification of critical Information Assets
- Understanding, with the help of IT and Business teams, the security weaknesses (vulnerabilities) and threats that may expose them to risk
- Analyzing the risks to determine priorities so that these risks can be managed

Vulnerability is the susceptibility to a negative event. For example, a person walking in the center of a highway is *vulnerable* to be run over by a vehicle.

Threat is an event which may exploit vulnerability. For example, an approaching bus may be a threat to the person who is walking in the center of a highway.

Risk is the probability that a threat may exploit a vulnerability to cause a negative impact. In the above example the risk is the possibility that a bus may run over the person walking in the center of the highway.

### Risk Management Process

The steps in carrying out Risk Management are:

- Risk Assessment

– Identification of assets

– Determination of critical assets

– Threat and vulnerability assessment of critical assets

– Risk quantification and prioritization

- Risk Treatment

– Risk treatment plan for the risks identified

– Tracking of risk treatment

Risk Assessment will be carried out at least once in a year. Risk Assessment may also need to be carried out on an ad-hoc basis, if there are major organizational or technological changes (e.g. corporate reorganization, redesign of the IT infrastructure or significant changes in the AR) or discovery of new threats or vulnerabilities based on security incidents inside or outside the enterprise. If required, the risk assessment can be taken up for a part of the organization (e.g. one or more department or asset) instead of the entire organization.

## Risk Assessment Steps

The steps to Risk Assessment are:

- Step 1: Asset Identification (*What is important?)*
- Step 2: Asset Valuation *(How critical is it?)*
- Step 3: Analysis of threats and vulnerabilities *(Where the problems are and how likely these problems to occur are?)*
- Step 4: Risk Assessment *(How serious are the problems?)*

The details of each of these steps are mentioned below:

### Step 1: Asset Identification

The aim of Step 1 is to identify the assets within the scope of the Risk Assessment. An inventory of assets will be produced of all identified assets in the form of an Asset Register (AR).

As part of this step, details of information-related assets will be collated in the form of an Asset Register. Examples of information-related assets, which will be considered for inclusion in the Asset Register, are:

- All proprietary information belonging to company
- All information relating to employees of company
- All supplier, contractor, customer and other third party information held by company
- All software assets such as application software, system software, development tools and utilities used in company
- All physical assets, such as computers, communications equipment, media, racks and equipment relating to facilities such as UPS, Batteries etc
- All information belonging to the any department in the form of hard and soft copies.
- All services, such as power, air conditioning, safety equipment, and security devices etc. associated with company's information systems
- People asset

Each manager will be responsible for compiling and maintaining the details of the information assets, pertaining to their areas of accountability. Individual asset users may also be required to compile or provide the details of information assets being used by them.

The Asset Register will include the following details:

- Department *(the department, which uses the asset)*
- Asset Name *(the name of the asset)*
- Asset Description *(a brief description about the asset)*
- Asset ID *(any ID given to that asset by company)*

- Asset Type *(type of the asset e.g. hardware, system software, hard-copy, soft-copy etc.)*
- Asset Classification *(the classification of the asset as per company's Information Class definitions)*
- Asset Location *(the location of the asset)*
- Asset Owner *(a person responsible for the asset)*
- Asset User *(user(s) who use this asset in their job)*
- Storage Requirement (*any specific storage requirements e.g. under lock & key, encryption etc.)*
- Retention Period *(any specific retention requirements)*

To capture people assets headings of Asset Register (AR) may be customized according to Organization.

All information at CARNIVAL GROUP shall be classified under one of the following three categories:

- Restricted
- Confidential
- Internal Use

**Restricted** - Unauthorized disclosure of which could cause serious damage to the national security or national interest or cause serious embarrassment in its functioning. This classification should be used for highly important information and is the highest classification normally used.

**Confidential** - Unauthorized disclosure / use of which could cause serious damage to the organization. Unauthorized disclosure/use of which would not be in the best interest of the organization and/or its customers, e.g. design details, computer software (programs, utilities), documentation, organization personnel data, budget information etc. All other information which does not require any degree of protection against disclosure within the organization, e.g. operating procedures, policies and standards inter office memoranda etc. Any such document is not permitted/allowed to be removed from office until and unless approved by the approving authority.

**Internal use:** All other information assets which are used to perform business activity does not require any degree of protection against disclosure within the organization need to be made for Internal Use.

## Step 2: Asset Valuation

The aim of Step 2 is to identify how valuable the assets are for company's business, and what might happen if their security is compromised.

Each Asset identified in the Asset Register will be assigned a value (3=High, 2=Medium, 1=Low) for each of the following parameters.

- Confidentiality

- Integrity
- Availability

The objective of assigning a value to these parameters is to ascertain what might happen if the security is compromised, so that the importance of the asset for company can be determined. An explanation of these parameters and their values is given below:

- **Confidentiality ( C )**

*How much of confidentiality problem is it (i.e. if the confidentiality of the asset is compromised)?*

| | |
|---|---|
| High (3) | Contains private and confidential data that merit highest degree of attention and handling, is intended to be exchanged only between two entities or limited number of individuals. |
| Medium (2) | Contains data for internal use whose release or loss may not be detrimental to the organization's interest. |
| Low (1) | Contains internal use and public data whose unauthorized disclosure pertain no risk. |

- **Integrity ( I )**

*How much of an integrity problem is it (i.e. if the integrity of the asset is compromised)?*

| | |
|---|---|
| High (3) | This causes a serious problem with the accuracy and completeness of Information (e.g. billing information, financial records, software source codes) |
| Medium (2) | This causes a noticeable problem (e.g. some information relating to services provided to customers / employees being incomplete or inaccurate) |
| Low (1) | This causes only a negligible or minor problem (e.g. internal documents that have little influence on critical parts of company's business) / No Impact |

- **Availability ( A )**

*How much of availability problem is it (i.e. if the availability of the asset is compromised)?*

| | |
|---|---|
| High (3) | The asset needs to be available more than 90% of the time |
| Medium (2) | The asset needs to be available for more than 70% time. |
| Low (1) | The asset needs to be available for less than 40% of the time. |

The Department Heads will contribute their perspectives in assigning values to these parameters, for asset pertaining to their business units or processes. The Risk Assessment team will consolidate this information to select those assets that are most valuable to the organization (critical assets).

The formula that will be used for asset valuation is mentioned below.

Asset Criticality Rating = C + I + A

Each asset would have a criticality rating as above.

**Threshold Limit for Risk Assessment:**

The threshold of criticality would be defined as detailed below. When:

C + I + A = 9 OR MORE
OR
C + I + A < 9 but rank of either of C, I, A is 3

All assets considered as critical and will be subjected to risk assessment.

### Step 3: Analysis of Threats & Vulnerabilities

The aim of Step 3 is to identify the potential causes of harm to the assets i.e. the threats and vulnerabilities, how likely a threat can cause problem to the asset and what can be the potential impact

For each and every asset that is identified as critical as part of Step 2, the vulnerabilities and the preventive factors will be taken into account for the applicable threats.

List of threats under each of these groups that is applicable to company's Information Environment. Please note that all threats mentioned in this list may not be applicable to a particular asset.

While performing Risk Assessment Information Asset Owners/ Custodians and Information Asset Users shall extend help and provide information to identify the vulnerabilities and preventive controls in place. The vulnerabilities and the preventive factors will be documented in the Risk Assessment & Treatment Sheet.

The RA & RT Sheet will capture the following details for each and every critical asset group of company:

- Threats (the threat in consideration)
- Vulnerabilities / Preventive factors (the weaknesses and countermeasures in place)
- Likelihood (the probability of a threat may occur. This is to be measured as: 0=No likelihood, 1=Low, 2=Medium, 3=High)
- Consequences (the consequences if the threat occurs)
- Impact (the consequence of the threat for company's Information Assets. This is to be measured as: 0= No Impact, 1=Low, 2=Medium, 3=High)

An explanation of the likelihood of a threat occurring and the impact are mentioned below:

- **Likelihood**

What is the likelihood of a threat occurring?

| | |
|---|---|
| High (3) | Highly likely, almost certain, common (expected to occur in most circumstances or will probably occur in most circumstances) |
| Medium (2) | Likely, probable (could occur at some time) |
| Low (1) | Unlikely, infrequent, rarely happens (not expected to occur or may occur only in exceptional circumstances) |

Likelihood can be judged based on past experience, judgement, industry standard or statistics. An example of how likelihood can be measured is illustrated below:

**Example: threat related to External Hacking (hacker from outside to inside)**

| | |
|---|---|
| High | The threat of the hacker gaining unauthorized access into the system is highly likely because there is a lot to gain and/or there is no protection in place |
| Medium | The threat of the hacker gaining unauthorized access into the system is likely because there is something to gain and/or the protection in place is not sufficient |
| Low | The threat of the hacker gaining unauthorized access into the system is unlikely because adequate protection measures are in place. |

- **Impact**

What would be the impact of the threat?

| | |
|---|---|
| High (3) | Would severely affect the reputation or interests of company |
| Medium (2) | Moderate impact on company's information assets or moderately affect reputation |
| Low (1) | Would threaten the efficiency or effectiveness of processes |

Impact can be realised in terms of direct or indirect losses including time, functionality, reputation and non-compliance.

**Key questions for this step**

- What, When, Where, Why and How threats are likely to occur and impact whom?
- What controls already exist to prevent threat from occurring?
- What are the current vulnerabilities and preventive factors?
- What is the likelihood of threats with the existing controls in place?
- What are the potential consequences if the threat occurs?

### Step 4: Risk Assessment

The aim of Step 4 is to assess the risks, based on the results of the previous steps.

The level of risk to each of the asset group will be determined using the results from the previous step:

Risk = Likelihood X Impact

**Likelihood** - Indicates the probability of the threat occurring. This is a function of the inherent vulnerabilities in the environment and the existing mitigation for the threats. Specific weaknesses which exist, in spite of the mitigating factors have to be taken into consideration as well. The likelihood of the threat occurring will be stated in levels 1 to 3 with 1 being the lowest probability of the threat occurring. In case the threat is not applicable, the likelihood will be 0.

**Impact** - Indicates impact of the threat on company. Impact states how much the process dependent upon the Information Assets will be affected if the threat occurs. The impact of the threat occurring will be stated in levels 0 to 3 with 0 being no impact and 3 being the highest impact.

## Risk Assessment Rating

The risk assessment carried out in accordance with the above will yield risk ratings from 0 to 9. The risk levels have been classified as follows:

| Sr. | Risk Levels | Classification |
|---|---|---|
| 1. | 0- 4 | Low |
| 2. | 6 | Medium |
| 3. | 9 | High |

All the resulting risks are uniformly classified in accordance with the above colour coding scheme to indicate the severity of the risks in each Risk Assessment Sheet.

## Risk Treatment

Depending on the risk assessment result, the areas of risk to be managed will be identified based on the degree of the risk. For the risks rated Medium and High, a Risk Treatment plan will be prepared. The Information Security Steering Committee and Information Security Forum will review the proposed risk treatment strategy and mitigation plans and refine them as appropriate.

Based on the risk assessment, all high and medium risks have to be included in the Risk Treatment Plan. The risks can be treated as follows:

- Mitigate the risks by identifying and implementing suitable controls

- Transfer the risk by insuring the assets
- Accept the risks

## Risk Acceptance

The risks identified, as part of risk assessment exercise will be taken as acceptable level of risk only if either of the following criteria is met:

- The Unit Information Security Committee perceives that the cost of control or effectively mitigating the risk is greater than the risk. E.g. shifting an entire factory to a location which is fewer earthquakes prone.
- The risk is going to be nullified / mitigated in the near future due to change in control environment or operating environment.
- Risks beyond the control of company management and are primarily of National / global nature
- Implementation of control might create concerns regarding safety of employees and / or humans in the neighbourhood.
- The control impedes the operations

## Reference

Asset Register
List of Threats
Risk Assessment and Risk Treatment Sheet
Residual Risk Approval Sheet

**User Awareness Policy:**

**Purpose**

The purpose of User Guidance is to describe the method of using the IT assets by the designated users and understanding their corresponding responsibilities to avoid any planned or unplanned incidents.

**Scope**

The Scope of this Methodology covers all the IT assets used in CARNIVAL GROUP.

**Introduction**

**STANDARDS STATEMENT**

The focus of user awareness towards Information Technology at CARNIVAL GROUP is aimed at creating an attitude towards a commitment to good security practices and facilitating a climate that sees IT security rules as beneficial to the protection of the business environment. The Information Technology team is responsible for all aspects of a user's security, usage awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.

**Information Technology Awareness Training Program**

The IT security awareness program blends formal training with periodic reminders and promotional materials to increase the understanding of vulnerabilities and threats to the University's information systems. Information security training is directed on improving the security skills and competencies of users.

### User Training Requirements

All users must participate in the awareness program through training sessions that correspond to role, responsibilities and use of information technology resources. This requirement is a condition of use.

A User Awareness Policy is a careful way towards the use of IT assets in terms of security, flexibility.

A User awareness Policy involves:

- Process of using IT Assets
- Understanding, with the help of IT team, the probable security weaknesses (vulnerabilities) and threats and the proactive approach to avoid them

### IT Training Trainings

Formal trainings with specific content designed to address specific IT Security Roles. The trainings are repeated annually at a minimum. Training content is reviewed annually to reflect changes in the IT security environment. Attendance at these trainings is recorded.

### General Security Awareness/Initial Account Training

This training is expected to increase user understanding and sensitivity to threats, vulnerabilities, and the need to protect company's personal information. All users are required to receive this training.

### Asset Usage Training

This training is expected to refresh user understanding and sensitivity towards the usage of Official and Unofficial IT assets as the devices are bonded with all sort of confidential and official information. All users are required to receive this training to make the IT environment more hassle free.

### Employee Security Awareness Training

This training provides an overview of compliance and is designed to explain employee responsibilities to security. Attention to IT Security policy and standards is provided with special focus on handling of sensitive data. This training is usually delivered on-line through e-mail/ publishing on IT portal and is tied to IT management process.

### Remote Users Security Training

This training provides an overview of employee responsibilities when connecting to information resources from a remote location. Attention to IT Security policy and standards, securing the workstation, handling of sensitive data and incident reporting is provided. This training is usually delivered on-line and is tied to VPN account management process.

### Disaster Recovery training

This training provides instruction on the policies and procedures related to the IT Disaster Recovery plan. It is designed to prepare the users to face and overcome to a certain level in case of any disaster/ incidents.

### IT Security Administrator Training

Training for those who manage, administer, operate, and design IT systems, is provided annually as practicable and necessary.

### New Employee Orientation

Basic information and training materials are provided to new employees as a part of their orientation to the IT department. This is an in person training where a formal guidelines are being taught to the user by the IT personnel.

### Security Review and Consultation

This is review session where Staff from the IT will be available to consult with company users on risk assessments, application reviews, vulnerability scans, rights managements and information on security best practices.

### Cyber Security Event

This is a proactive training to raise awareness about cyber security and online safety by highlighting precautions users can take to help protect themselves online. Continuous notification are being sent to users through e-mail on educating the ongoing/ newly coming cyber threats to avoid any sort of online hassles.

## Defined User Responsibilities of CARNIVAL GROUP:

- User is responsible and accountable for safeguarding and monitoring of assets against unauthorized disclosure, modification, destruction or loss of availability for any asset issued from CARNIVAL GROUP stores.
- User is prohibited to install any third party, restricted software on any CARNIVAL GROUP owned machine without prior approval from IT Head and concerned department.
- When good judgment has not been exercised in safeguarding a portable computing device, the individual may be subject to disciplinary action and be held responsible for the replacement cost if the device is lost or stolen.
- Paper documents containing Business Critical Information must be filed or locked away when not in use.
- CARNIVAL GROUP reserves the right to monitor content and traffic and to electronically screen networking and computing resources for all activity using CARNIVAL GROUP electronic messaging, or network and computing resources.
- No changes to the security settings or configuration of any approved device can be made without prior authorization from IT department.

- User is responsible for the backup of critical and important data, a cloud backup storage (through online agent) shall be provided to keep a copy of the same at user's request for regular backup.
- Personally- owned computing Devices are prohibited from connecting to and accessing CARNIVAL GROUP NETWORK, either directly or via remote access until approved by user department head, IT head & Head Operations.
- Users shall not disable any security software e.g. automated virus scanning or firewall.

## Change Management Policy:

### Purpose

The purpose of User Guidance is to describe the method of recording and reviewing all the IT related changes either hardware or Software.

### Scope

The Scope of this Methodology covers all the IT assets used in CARNIVAL GROUP.

### Introduction

**STANDARDS STATEMENT**

The focus of change management towards Information Technology at CARNIVAL GROUP is aimed at creating an attitude towards a commitment to good security practices and facilitating a climate that sees IT security rules as beneficial to the protection of the business environment. The Information Technology team is responsible for all changes on all assets.

A change management Policy involves:

- The process for all planned activities.
- The process for all un-planned activities.

**Process Flow for any planned changes in Technical Environment**

**Activities covered:**

1. Any technical activities that has a change impact in any ongoing configuration or process, such as:
   a. Any Type of configuration change in any server firm
   b. Any type of configuration changes in any network firm
   c. Any type of configuration changes in any security firm
   d. Any type of changes in any broadcast firm
   e. Any new technology implementation.
   f. Pushing of any updates to any network.

**Process Flow:**

Step-1: Pre approval:

a. Before any changes please notify to the concerned authority through e-mail about the forth coming activity.
b. Create a testing environment.
c. Post testing notify to the concerned authority with the testing results through e-mail.

Step-2: CMR (Change Management request)

a. Upon receiving written approval submit the change management form (CMR)
b. Post acceptance of the CMR form by the concerned authority implement the changes.

Step-3: Failed Testing/ CMR:

a. In case of any fall back, written intimations should be sent to the concerned authority.
b. RCA (Root cause analysis) need to be sent in case of any failed testing.

***NB: All the above forms need to be approved through soft copy (on e-mail) and also on Hard copy (physical Paper).

### Process Flow for any Un-planned changes in Technical Environment

Activities Covered:

1. All types of unplanned/ uncertain changes such as:
    a. Sudden failure in any server firm
    b. Sudden failure in any network firm
    c. Sudden failure in any broadcast firm

### Process Flow:

1. Immediately intimate the concerned authority through Phone Call/ SMS
2. Seek and suggest the technical changes need to be taken to overcome the failure with proper approval.
3. Commit the changes.
4. Validate the changes and intimate the concerned authority again on the result of the changes
5. Float an e-mail to the concerned people/ team
6. On successful result prepare a RCA (Root Cause Analysis) and float it to the concerned authorities through e-mail.

Sample Forms:

Change Management:

# Change and Impact Analysis Form

| | |
|---|---|
| **Change And Impact Analysis Form** | |
| Change Request No. | **NOD/IT/xxx** |
| Details of Change Required | |
| Requested By | |
| Requestors signature | |
| Date when Raised | |
| Contact Details (ph and email) | |
| Unit / Department/ Location | |
| Change Requirement (please mention validity if requesting a temporary change) | |
| Reasons/Benefits/Business Purpose | |
| Priority (Normal/Emergency) (Target Timeline if any) | |
| Additional Comments | |
| Impacted System Details | |
| Time Impact ( Estimated Time) | |
| Service Downtime if any | |
| Cost Impact | |
| Complexity | |
| Risks | |
| Impact of not carrying out Change | |

| | **Name** | **Designation** | **Date** | **Signature** | **Remarks** |
|---|---|---|---|---|---|
| Initiator | | | | | |
| Approver | | | | | |
| Closure of Request | | | | | |

Root Cause Analysis:

# Security/Incident Form

| | | | |
|---|---|---|---|
| Record No | Carnival/MUM/xxx | | |
| From | | To | |
| Remark | All time IST | | |

| | | | | |
|---|---|---|---|---|
| A | DETAILS OF SECURITY INCIDENT | | | |
| | **Incident:**<br>**Departments Affercted:**<br>**Users Impacted:**<br>**Downtime Minutes:**<br>**Impact (Complete/Partial): Complete:**<br>**Ping and Tracert:**<br>**Tickets raised Internally:**<br>**Production Outage:**<br>**Chronology of the Events:** | | | |
| | Reported/Identified by | | Designation | |
| | Signature | | Date | |
| B | ROOT CAUSE ANALYSIS | | | |
| | | | | |
| C | CORRECTIVE ACTION | | | |
| | | | | |
| | | | | |
| D | PREVENTIVE ACTION | | | |
| | | | | |
| | Name | | Designation | |
| | Signature | | Date | |
| E | Learning from security incident | | | |
| | | | | |
| Verified By | | | Designation | |
| Signature | | | Date | |
| Reviewed By HOD | | | Comments | |
| Signature of HOD | | | Date | |