



Security Policy and Processes

United States Global Headquarters

4899 Belfort Road
Suite 400
Jacksonville, FL 32256

PO Box 1559
Ponte Vedra Beach, FL 32004

O: 904-766-1600 | F: 407-393-5517 | us@ocenture.com

Table of Contents

Ethics Policy	3
Information Sensitivity	5
Acceptable Use Policy.....	7
Remote Access Policy.....	10
Email Use Policy	12
Email Retention Policy	14
Guidelines on Antivirus Process.....	16
Server Security Policy	17
Password Policy.....	19
Database Password Policy.....	22
Encryption Policy	24
Risk Assessment Policy	25
Access Control Policy	26
Information Security Policy.....	28
Risk Management Processes	30
Management Change Guidelines.....	34
Approvals, Revisions and Adjustments	37

Ethics Policy

1. Overview

Ocenture's purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Ocenture employee. All Ocenture employees, partners and vendors are required to familiarize themselves with the ethics guidelines that follow this introduction.

Ocenture is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. By addressing issues proactively and using correct judgment in all our business practices we set ourselves apart from our competitors.

Ocenture does not tolerate any wrongdoing or impropriety at anytime. Ocenture will take the appropriate measures to act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2. Purpose

Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy serves to guide our business behavior and to ensure companywide ethical conduct.

3. Scope

This policy applies to employees, contractors, consultants, temporaries, partners and other workers at Ocenture, including all personnel affiliated with third parties.

4. Policy

4.1. Executive Commitment to Ethics

- 4.1.1. Top brass within Ocenture will lead by example. Ocenture's business practice, honesty and integrity is held as one of the companies to top priorities.
- 4.1.2. Ocenture utilizes an open door policy to welcome suggestions and concerns from employees. Our open door policy allows employees to feel comfortable discussing any issues and will provide an advance alert system to any problems within the work force.
- 4.1.3. Ocenture executives will disclose any conflict of interests in regard to employee positions.

4.2. Employee Commitment to Ethics

- 4.2.1. Ocenture employees must treat everyone fairly, have mutual respect and promote a team environment and avoid the intent of unethical or compromising practices.
- 4.2.2. Every employee is required to apply effort and intelligence in maintaining ethics value.
- 4.2.3. Employees will disclose any conflict of interests in regard to their position within Ocenture.
- 4.2.4. Employees will help Ocenture to increase customer and vendor satisfaction by providing quality services and timely responses to inquiries.

4.3. Company Awareness

- 4.3.1. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.
- 4.3.2. Ocenture promotes a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. Maintaining Ethical Practices

- 4.4.1. Ocenture reinforce through employee meetings the importance of the integrity and supporting coworkers. Every employee, manager, director consistently maintains an ethical stance and support ongoing ethical behavior.
- 4.4.2. Employees at Ocenture encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.
- 4.4.3. Ocenture has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.5. **Unethical Behavior**

- 4.5.1. Ocenture will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.
- 4.5.2. Ocenture will not tolerate harassment or discrimination.
- 4.5.3. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.
- 4.5.4. Ocenture will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

5. **Enforcement**

- 5.1. Any infractions of this code of ethics will not be tolerated and Ocenture will act quickly in correcting the issue if the ethical code is broken.
- 5.2. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

Information Sensitivity

1. Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Ocenture without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All Ocenture are required to familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Ocenture Confidential information (e.g., Ocenture Confidential information should not be left unattended in conference rooms).

2. Scope

All Ocenture information is categorized into two main classifications:

- Ocenture Public
- Ocenture Confidential

Ocenture Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Ocenture.

Ocenture Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that is protected very closely, such as trade secrets, development programs, potential acquisition targets, suppliers, partnerships and other information integral to the success of our company. Also included in Ocenture Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc.

A subset of Ocenture Confidential information is "Ocenture Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Ocenture by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, partnership agreements, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Ocenture's network to support our operations. Ocenture personnel are encouraged to use common sense judgment in securing Ocenture Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact management.

3. Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Ocenture employees use these guidelines as a reference point to protect company data, as Ocenture Confidential information in each category may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Ocenture Confidential information in question.

3.1. Minimal Sensitivity: General corporate information; some personnel and technical information.

3.1.1. Access: Ocenture employees, contractors, people with a business need to know.

- 3.1.2. **Distribution within Ocenture:** Standard interoffice mail, approved electronic mail and electronic file submission.
 - 3.1.3. **Distribution outside of Ocenture internal mail:** U.S. mail and other public or private carriers approved electronic mail and electronic file transmission methods.
 - 3.1.4. **Electronic distribution:** No restrictions except that it is sent to only approved recipients.
 - 3.1.5. **Distribution within Ocenture:** Standard interoffice mail, approved electronic mail and electronic file transmission methods.
 - 3.1.6. **Storage:** Ocenture employees are required to keep any document from view of unauthorized people; erase whiteboards as required, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
 - 3.1.7. **Disposal/Destruction:** Deposit outdated paper information in specially marked disposal / shred bins on Ocenture premises; electronic data should be expunged / shredded / cleared. Reliably erase or physically destroy media.
 - 3.1.8. **Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.
- 3.2. **More Sensitive:** Business, financial, technical, and most personnel information.
- 3.2.1. **Access:** Ocenture employees and non-employees with signed non-disclosure agreements who have a business need to know.
 - 3.2.2. **Distribution within Ocenture:** Standard interoffice mail approved electronic mail and electronic file transmission methods.
 - 3.2.3. **Distribution outside of Ocenture internal mail:** Sent via U.S. mail or approved private carriers.
 - 3.2.4. **Electronic distribution:** No restrictions to approved recipients within Ocenture, this data must be encrypted using PGP or sent via a private link to approved recipients outside of Ocenture premises.
 - 3.2.5. **Storage:** Individual access controls are required by all employees for electronic information.
 - 3.2.6. **Disposal/Destruction:** In specially marked disposal bins and shredders on Ocenture premises; electronic data will be expunged / cleared / shredded. Reliably erase or physically destroy media.
 - 3.2.7. **Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.
- 3.3. **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company.
- 3.3.1. **Access:** Only those individuals (Ocenture employees and non-employees) designated with approved access and signed non-disclosure agreements.
 - 3.3.2. **Distribution within Ocenture:** Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
 - 3.3.3. **Distribution outside of Ocenture internal mail:** Delivered direct; signature required; approved private carriers.
 - 3.3.4. **Electronic distribution:** No restrictions to approved recipients within Ocenture, however it is required that all information be strongly encrypted using PGP.
 - 3.3.5. **Storage:** Individual access controls are required for electronic information. Physical security is used, and information will be stored in a physically secured computer.
 - 3.3.6. **Disposal/Destruction: Strongly Encouraged:** In specially marked disposal bins on Ocenture premises; electronic data will be expunged / shredded / cleared. Reliably erase or physically destroy media.
 - 3.3.7. **Penalty for deliberate or inadvertent disclosure:** Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

Acceptable Use Policy

1. Overview

Ocenture's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Ocenture's established culture of openness, trust and integrity. Ocenture is committed to protecting Ocenture's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Ocenture. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Ocenture employee and affiliate who deals with information and/or information systems. It is required that every computer user to know these guidelines, and conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Ocenture. These rules are in place to protect the employee and Ocenture. Inappropriate use exposes Ocenture to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Ocenture, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Ocenture.

4. Policy

4.1. General Use and Ownership:

- 4.1.1. While Ocenture's network administration provides a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Ocenture. Because of the need to protect Ocenture's network, management will not guarantee the confidentiality of information stored on any network device belonging to Ocenture.
- 4.1.2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments have created guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees will be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
- 4.1.3. Ocenture requires that information a user considers sensitive or vulnerable be encrypted. For guidelines on information classification, see Ocenture's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Ocenture's Awareness Initiative.
- 4.1.4. For security and network maintenance purposes, authorized individuals within Ocenture will monitor equipment, systems and network traffic at any time, per Ocenture's Audit Policy.
- 4.1.5. Ocenture reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2. Security and Proprietary Information:

- 4.2.1. The user interface for information contained on Internet/Intranet/Extranet-related systems will be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential

information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees are required to take the necessary steps to prevent unauthorized access to this information.

- 4.2.2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords must be changed quarterly; user level passwords will be changed every six months.
- 4.2.3. All PCs, laptops and workstations are required to be secured with a password-protected screensaver with the automatic activation feature set at 5 minutes or less, or by logging-off when the host will be unattended.
- 4.2.4. All Ocenture employees will use PGP encryption of information in compliance with Ocenture's Acceptable Encryption Use policy.
- 4.2.5. Postings by employees from an Ocenture email address to newsgroups must contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Ocenture, unless posting is in the course of business duties.
- 4.2.6. All hosts used by the employee that are connected to the Ocenture Internet/Intranet/Extranet, whether owned by the employee or Ocenture, must be continually executing approved virus scanning software with a current virus database. Unless overridden by departmental or group policy.
- 4.2.7. Employees are required to use extreme caution when opening e-mail attachments, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

- 4.3.1. The following activities are prohibited. Employees are exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
- 4.3.2. Under no circumstances is an employee of Ocenture authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Ocenture-owned resources.

4.4. System and Network Activities

- 4.4.1. The following activities are strictly prohibited, with no exceptions: Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Ocenture.
- 4.4.2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Ocenture or the end user does not have an active license is strictly prohibited.
- 4.4.3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- 4.4.4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- 4.4.5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- 4.4.6. Using an Ocenture computing asset to actively engaged in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- 4.4.7. Making fraudulent offers of products, items, or services originating from any Ocenture account.
- 4.4.8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- 4.4.9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

- 4.4.10. Port scanning or security scanning is expressly prohibited unless prior notification to Ocenture is made.
- 4.4.11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- 4.4.12. Circumventing user authentication or security of any host, network or account.
- 4.4.13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- 4.4.14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- 4.4.15. Providing information about, or lists of, Ocenture employees to parties outside Ocenture.

4.5. **Email Communications Activities**

- 4.5.1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- 4.5.2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- 4.5.3. Unauthorized use, or forging, of email header information.
- 4.5.4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- 4.5.5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- 4.5.6. Use of unsolicited email originating from within Ocenture's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Ocenture or connected via Ocenture's network.
- 4.5.7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5. **Enforcement**

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

6. **Definitions**

Spam

Unauthorized and/or unsolicited electronic mass mailings.

Remote Access Policy

1. Purpose

The purpose of this policy is to define standards for connecting to Ocenture's network from any host. These standards are designed to minimize the potential exposure to Ocenture from damages which may result from unauthorized use of Ocenture resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Ocenture internal systems, etc.

2. Scope

This policy applies to all Ocenture employees, contractors, vendors, agents and partners with a computer or workstation used to interact with the Ocenture network. This policy applies to remote access connections used to do work on behalf of Ocenture, including reading or sending email and viewing intranet web resources.

3. Policy

3.1. General

3.1.1. It is the responsibility of Ocenture employees, contractors, vendors, partners and agents with remote access privileges to Ocenture's corporate network resources to ensure that their remote access connection is given the same consideration as the user's on-site connection to Ocenture resources.

3.1.2. Please review the following policies for details of protecting information when accessing the corporate network resources via remote access methods, and acceptable use of Ocenture's network.

- Acceptable Encryption Policy
- Acceptable Use Policy

3.2. Requirements

3.2.1. Secure remote access will be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

3.2.2. At no time should any Ocenture employee provide their login or email password to anyone, not even family members.

3.2.3. Ocenture employees and contractors with remote access privileges are required to ensure that their Ocenture-owned or personal computer or workstation, which is remotely connected to Ocenture's corporate network resources, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

3.2.4. Ocenture employees and contractors with remote access privileges to Ocenture's corporate network must not use non-Ocenture email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Ocenture business, thereby ensuring that official business is never confused with personal business.

3.2.5. All hosts that are connected to Ocenture internal networks via remote access technologies must use the most up-to-date anti-virus software (see IT Manager), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

3.2.6. Personal equipment that is used to connect to Ocenture's network resources must meet the requirements of Ocenture-owned equipment for remote access.

3.2.7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Ocenture production network must obtain prior approval.

4. **Enforcement**

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or termination of partner agreement.

5. **Definitions**

Dual Homing

Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on an Ocenture-provided Remote Access home network, and connecting to another network, such as a spouse's remote access.

Remote Access

Any access to Ocenture's corporate network through a non-Ocenture controlled network, device, or medium.

Split-tunneling

Simultaneous direct access to a non-Ocenture network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Ocenture's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

Email Use Policy

1. Purpose

To prevent tarnishing of the Ocenture brand(s) when email is sent to the general public. The general public will view these messages as an official policy statement from an Ocenture staff member.

2. Scope

This policy covers appropriate use of any email sent from an Ocenture email address and applies to all employees, vendors, and agents operating on behalf of Ocenture.

3. Policy

3.1. Prohibited Use

3.1.1. The Ocenture email system will not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Ocenture employee should report the matter to their supervisor immediately.

3.2. Personal Use

3.2.1. Using a reasonable amount of Ocenture resources for personal emails is acceptable, but non-work related email will be saved in a separate folder from work related email. Sending chain letters or joke emails from an Ocenture email account is strictly prohibited. These restrictions also apply to the forwarding of mail received by an Ocenture employee.

3.3. Monitoring

3.3.1. Ocenture employees will have no expectation of privacy in anything they store, send or receive on the company's email system. Ocenture may monitor messages without prior notice. Ocenture is not obliged to monitor email messages.

3.4. Virus Warnings

3.4.1. Occasional warnings, updates and precautionary procedures will be sent to Ocenture Employees by IT Management. Such correspondence will give directive instructions for new threats and reporting suspicious computer behavior in relation to new viruses. Each employee is expected to follow the guidelines and procedures outlined in such correspondence. Any suspected virus threats should be reported immediately to IT Management.

4. Enforcement

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

5. Definitions

Email

The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.

Forwarded email

Email resent from an internal network to an outside point.

Chain email or letter

Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Sensitive information

Information is considered sensitive if it can be damaging to Ocenture or its customers' reputation or market standing.

Virus Warning

Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

Unauthorized Disclosure

The intentional or unintentional revealing of restricted information to people, both inside and outside Ocenture, who do not have a need to know that information.

Email Retention Policy

1. Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees are required to familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to IT Management.

2. Scope

All Ocenture email information is categorized into four main classifications with retention guidelines:

Administrative Correspondence (4 years)

Fiscal Correspondence (4 years)

General Correspondence (1 year)

Ephemeral Correspondence (Retain until read, destroy)

3. Policy

3.1. Administrative Correspondence

3.1.1. Ocenture Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only will be treated as Administrative Correspondence. To ensure Administrative Correspondence is retained, a mailbox admin@ocenture.com has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.2. Fiscal Correspondence

3.2.1. Ocenture Fiscal Correspondence is all information related to revenue and expense for the company. To ensure Fiscal Correspondence is retained, a mailbox fiscal@ocenture.com has been created, if you copy (cc) this address when you send email, retention will be administered by the IT Department.

3.3. General Correspondence

3.3.1. Ocenture General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4. Ephemeral Correspondence

3.4.1. Ocenture Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5. Encrypted Correspondence

3.5.1. Ocenture encrypted communications must be stored in a manner consistent with Ocenture Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

4. **Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. **Definitions**

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. If you have a business need to use other mailers contact the appropriate support organization

Individual Access Control

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command. On Mac's and PC's, this includes using passwords on screensavers.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Ocenture.

Encryption

Secure Ocenture Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

Guidelines on Antivirus Process

Recommended processes to prevent virus problems:

1. Ocenture computer systems all support up-to-date anti-virus software that is installed on every computer. The Ocenture IT Department will run daily a current version; the IT Department will download and install anti-virus software updates as they become available.
2. NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
3. Delete spam, chain, and other junk email without forwarding, using the Ocenture's *Acceptable Use Policy*.
4. Never download files from unknown or suspicious sources.
5. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
6. Back-up critical data and system configurations on a regular basis and store the data in a safe place.
7. New viruses are discovered almost every day. Periodically IT Management will send routine emails for security updates with cautions, warnings or upgrade requirements.
8. Each employee is expected to notify IT Management of any suspicious computer malfunctions via in person or through corporate email.

Server Security Policy

1. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and / or operated by Ocenture. Effective implementation of this policy will minimize unauthorized access to Ocenture proprietary information and technology.

2. Scope

This policy applies to server equipment owned and/or operated by Ocenture, and to servers registered under any Ocenture-owned internal network domain.

This policy is specifically for equipment on the internal Ocenture network. For secure configuration of equipment external to Ocenture, refer to the hosted partner appendix *Rack Space Managed Hosting*.

3. Policy

3.1. Management and Responsibilities

3.1.1. All internal servers deployed at Ocenture are managed by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by Ocenture management. Operational groups monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group has established a process for changing the configuration guides, which includes review and approval by Ocenture management.

3.1.2. Servers are registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact.

Server contact(s) and location, and a backup contact
 Hardware and Operating System/Version
 Main functions and applications, if applicable

3.1.3. Information in the corporate enterprise management system are be kept up-to-date and monitored by the operational group.

3.1.4. All configuration changes for production servers follow the appropriate change management procedures.

3.2. General Configuration Guidelines

3.2.1. Operating System configuration are kept in accordance with approved Ocenture guidelines.

3.2.2. Services and applications that will not be used must be disabled where practical.

3.2.3. Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.

3.2.4. The most recent security patches are maintained and installed on all systems as soon as practical, the only exception being when immediate application would interfere with business requirements.

3.2.5. Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.

3.2.6. Always use standard security principles of least required access to perform a function.

3.2.7. Do not use root when a non-privileged account will do.

3.2.8. If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).

3.2.9. All servers are physically located in an access-controlled environment.

3.2.10. All servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3. **Monitoring**

- 3.3.1. All security-related events on external critical or sensitive systems are logged by Co-located Hosting Service.

Rack Space Managed Hosting
Annual Report on Controls available upon approval

3.4. **Compliance**

- 3.4.1. Audits are performed on a regular basis by authorized organizations through Ocenture.
- 3.4.2. Audits are managed by the internal audit group or management, in accordance with the *Audit Policy*. Management will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.
- 3.4.3. Every effort is made to prevent audits from causing operational failures or disruptions.

4. **Enforcement**

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

5. **Definitions**

Server

For purposes of this policy, a Server is defined as an internal / external Ocenture Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

Password Policy

1. Purpose

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password can result in the compromise of Ocenture's entire corporate network. As such, all Ocenture employees (including contractors and vendors with access to Ocenture systems) are required to take the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Scope

The scope of this policy includes all personnel and partners who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Ocenture facility, has access to the Ocenture network, or stores any non-public Ocenture information.

3. Policy

3.1. General

- 3.1.1. All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- 3.1.2. All production system-level passwords must be part of the Otrack administered global password management database.
- 3.1.3. All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- 3.1.4. User accounts that have system-level privileges granted through group memberships or programs such as "Super Admin" must have a unique password from all other accounts held by that user.
- 3.1.5. Passwords must not be inserted into email messages or other forms of electronic communication.
- 3.1.6. All user-level and system-level passwords must conform to the guidelines described below.
- 3.1.7. All passwords must be at least 8 characters, include both alpha and numeric characters, and include one capital letter with a special character. (for example: tree28&House)

3.2. Guidelines

- 3.2.1. **General Password Construction Guidelines:** Passwords are used for various purposes at Ocenture. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

The password contains less than eight characters.
 The password is a word found in a dictionary (English or foreign).
 The password is a common usage word such as

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret).
- The words "Ocenture", "jacksonville", "jax", "California", "CA",
- Or any derivation of common Ocenture street addresses or numbers.

Strong passwords have the following characteristics:

Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have 8 digits and punctuation characters as well as letters e.g., 0-9,!,%,(),_+,=,{}[],
- Are at least eight alphanumeric characters long.
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Note: Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

3.3. Password Protection Standards

- 3.3.1. Do not use the same password for Ocenture accounts as for other non-Ocenture access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Ocenture access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.
- 3.3.2. Do not share Ocenture passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Ocenture information.

Here is a list of "donts":

- Don't reveal a password over the phone.
- Don't reveal a password in an email message
- Don't reveal a password to the employer, management or executive staff member
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

- 3.3.3. If someone demands a password, refer them to this document or have them contact the IT Department.
- 3.3.4. Do not use the "Remember Password" feature of applications (e.g., Eudora, Out-Look, Netscape Messenger).
- 3.3.5. Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption or password protection.
- 3.3.6. Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.
- 3.3.7. If an account or password is suspected to have been compromised, report the incident to the IT Manager and change all passwords immediately.
- 3.3.8. Password cracking or guessing may be performed on a periodic or random basis by the IT Staff or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

3.4. Application Development Standards

Application developers are required to ensure their programs contain the following security precautions. Applications:

- 3.4.1. Support authentication of individual users, not groups.
- 3.4.2. Ocenture systems will not store passwords in clear text or in any easily reversible form.

3.4.3. All systems will provide role management, such that one user can take over the functions of another without having to know the other's password.

3.5. Use of Password and Pass phrases for Remote Access Users

Access to the Ocenture Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase.

3.6. Pass phrases

Access to the Ocenture Networks via remote access is controlled using either a one-time password authentication or a public/private key system with a strong pass phrase.

3.6.1. Pass phrases are used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

3.6.2. Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks".

3.6.3. A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.

Note: All of the rules above that apply to passwords apply to pass phrases.

4. Enforcement

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

5. Definitions

Application Administration Account

Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

Database Password Policy

1. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Ocenture's networks.

Computer programs running on Ocenture's networks often require the use of one of the many external database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

2. Scope

This policy applies to all software that will access an Ocenture, multi-user production database.

3. Policy

3.1. General

3.1.1. In order to maintain the security of Ocenture's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be publicly accessed through a web server.

3.2. Specific Requirements

3.2.1. Storage of Data Base User Names and Passwords

3.2.1.1. Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable.

3.2.1.2. Database credentials may reside on the database server. In this case, a hash number identifying the credentials may be stored in the executing body of the program's code.

3.2.1.3. Database credentials may not reside in the documents tree of a web server.

3.2.1.4. Passwords must not be stored in 'Outlook' or any other software not authorized by Ocenture.

3.2.1.5. Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

3.2.2. Retrieval of Database User Names and Passwords

3.2.2.1. If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

3.2.2.2. The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

3.2.3. Access to Database User Names and Passwords

3.2.3.1. Every program or every collection of programs implementing a single business function must have database username and passwords located outside of root directory and stored into secure directory (i.e., root/config/access).

3.2.3.2. Database passwords used by programs are system-level passwords as defined by the *Password Policy*.

3.2.3.3. Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

3.2.4. Coding Techniques for implementing this policy

3.2.4.1. Site-specific guidelines for the different coding languages include, but not limited to, PHP, MySQL and JavaScript.

4. Enforcement

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

5. Definitions

Computer language

A language used to generate programs.

Credentials

Something you know (e.g., a password or pass phrase), and/or something that identifies you (e.g., a user name, a fingerprint, voiceprint, retina print). Something you know and something that identifies you are presented for authentication.

Executing Body

The series of computer instructions that the computer executes to run a program.

Production

Software that is being used for a purpose other than when software is being implemented or tested.

Entitlement

The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.

Encryption Policy

1. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2. Scope

This policy applies to all Ocenture employees, affiliates and partners.

3. Policy

Proven, standard algorithms such as DES, Blowfish, RSA, PGP, RC5, AES/Rijndael and IDEA will be used as the basis for encryption technologies. Advanced Encryption Standard (AES) is the new governmental standard for encryption which was sanctioned for development by National Institute of Standards and Technology (NIST). These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Ocenture's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Ocenture.

4. Enforcement

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

5. Definitions

Proprietary Encryption

An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem

A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem

A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Risk Assessment Policy

1. Purpose

To empower IT management to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2. Scope

Risk assessments can be conducted on any entity within Ocenture or any outside entity that has signed a *Third Party Partner Agreement* with Ocenture. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3. Policy

The execution, development and implementation of remediation programs are the joint responsibility of management and the department responsible for the systems area being assessed. Employees are required to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the Risk Assessment Team in the development of a remediation plan.

4. Risk Assessment Process

For additional information; go to the Risk Assessment Report (TBA).

5. Enforcement

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

6. Definitions

Entity

Any business unit, department, group, or third party, internal or external to Ocenture, responsible for maintaining Ocenture assets.

Risk

Those factors that could affect confidentiality, availability, and integrity of Ocenture's key information assets and systems. Ocenture is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

Access Control Policy

1. Overview

This policy sets forth the requirement for access control of Ocenture information assets.

2. Purpose

The confidentiality, integrity and availability of information stored within the information systems of the Ocenture will be protected. Therefore, only authorized users can access specific information assets.

3. Scope

The scope of this policy includes all personnel and partners who have or are responsible for an account (or any form of access that supports or requires access to information systems) on any system that resides at any Ocenture facility, has access to the Ocenture network, or stores any non-public Ocenture information

4. Policy

4.1. General

4.1.1. **Controls Access** to its information assets in computer systems. Only authorized users shall be granted access. Authorized users shall be limited to specific defined, documented, and approved systems and applications, as determined by their level of access rights (i.e., role based access control).

4.1.2. **Access Authorization (Managers/Administrators):** Managers and Administrators will grant access to users based on what the user requires to accomplish their assigned duties. The Individual User Profile (IUP) forms shall be used for processing all requests.

4.1.3. **Access Approval (Users):** Information users will inform IT Manager/Administrator if access approved is not enough to carry out their assigned duties.

4.1.4. **Access Control Protection:** Electronic information assets will be protected through access controls, which prevent improper creation, disclosure, modification, deletion or data unavailability. Examples of access control systems include, but are not limited to, secured building areas, traditional system passwords, application validation, etc., as well as other access control technologies.

4.1.5. **Consistent Protection:** Access controls shall be applied consistently to electronic information assets throughout their life cycle, from origination to destruction.

4.2. Guidelines and Responsibilities

4.2.1. Managers evaluate each information user's access to verify their continued need for assigned access level whenever work assignments change or at a minimum annually.

4.2.2. Managers immediately request revocation of access privileges when user leaves Ocenture or changes occur and user no longer requires the same access privileges.

4.2.3. The IT Manager maintains a list of managers having primary responsibility for information assets and the area of information assets to which their authority extends.

4.3. Access Privilege Revocation Assignment

4.3.1. The following circumstances require managers to request appropriate modification and/or revocation of access privileges to information assets and data systems.

4.3.2. When users are functioning outside of their current work assignments, modify and/or revoke access privileges.

4.3.3. During a user's extended leave, and/or when deemed appropriate by the Human Resources Office, revoke access privileges.

4.3.4. Termination of user from Ocenture, revoke all access privileges.

4.3.5. IT Managers assign unique, user identification to the authorized information user upon notification of access approval.

4.3.6. Information system applications authenticate all users, where applicable. Unauthorized users shall be denied access.

- 4.3.7. Automatic revocation of user access privileges occur after 180 days of non-logon to information systems or applications, where possible.
- 4.3.8. Unauthorized or wrongful use or disclosure of information assets may cause the immediate revocation of access based on the Ocenture acceptable use policy.

5. **Enforcement**

Any employee or partner found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or partner agreement.

Information Security Policy

1. Overview

It is important that Ocenture's information security programs, policies, and procedures required to be reviewed on a frequent basis to determine impacts to both Ocenture and the customer's protection of sensitive data.

2. Owners

This information policy review covers appropriate criteria of any email sent from an Ocenture email address and applies to all employees, vendors, and agents operating on behalf of Ocenture.

Step 1: Information Security Manager. Completes a one-page description and outline of the security policy content area to be reviewed / discussed.

Step 2: Management Review Board (MRB). Review the one-page description and outline. Recommend approval to begin development of the content area document(s).

Step 3: Document Author(s). One-third of the way through the development process, completes an initial draft of the document(s) using the Security Policy article template already established from Security Policy version 1.

Step 4: Management Review Board. Review the draft. Recommend acceptance / rejection.

Step 5: Document Author(s). Two-thirds of the way through the development process, submits document/policy to external reviewers.

Step 6: Reviewers. Review the draft. Note: At least two required reviewers are designated for each document.

Step 7: Document Author(s). Resolves all issues raised by reviewers and modifies the document accordingly. Note: If either a reviewer or the author feels that the requested changes are major, the document must undergo another review pass.

Step 8: Management Review Board. Recommend final acceptance/rejection.

Step 9: Technical Lead. Decides on final acceptance/rejection.

Step 10: Editor. Performs edit.

3. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4. Definitions

Information Security Manager

Responsible for the management and supervision of use of security measures to protect data, and conduct of personnel in relation to the protection of data.

Management Review Board

Comprised of high-level decision makers who review the purpose of policy, process and procedure in order to ensure the alignment of strategic business goals as they relate to Information Security best practices.

Document Authors

Individuals allocated the duty and responsibilities to identify the necessary changes and best practices to be implemented into policy in relation to Information Security.

Reviewers

Responsible for proof reading, reviewing, correcting and making suggestions for adequate publishing. This team is comprised of two or more members for cross-referencing and validation purposes.

Technical Lead

The authority on the policy content and owner of the review process.

Editor

Combines all corrections, revisions and changes to the policy in order to create a seamless document which becomes aligned with the master policy document.

Risk Management Processes

1. Purpose

The Risk Management Process defines the process the Ocenture Information Security Organization will employ to execute and identify information security risks as early as possible and to periodically reassess and manage those risks.

The process contained in this document defines elements of the information security risk management program. The process covers identifying risks, prioritizing, risk reduction techniques, risk contingency plans, identifying the measures to track risks, and implementing contingency plans, when required.

2. Scope

The Ocenture risk mitigation process is to track risks that could adversely impact mission critical data across the enterprise. The cornerstone of the methodology described in this document is early identification of potential risk / problems coupled with methods to reduce impacts. Identification is accomplished through an on-going pre-planned management review process. Program variances are identified early; corrective actions should be planned and implemented before a problem becomes major.

3. Roles and Responsibilities

The Risk Management Process applies to all business unit of Ocenture.

IT Manager

The IT Manager is responsible for managing the risks associated with the development and maintenance of the information security system and ensuring that risk management is performed in accordance with the processes described herein.

Risk Management Manger

The IT Manager has many responsibilities which include being the Risk Management Manager (RMM) specifically because of current IT staff size. Otherwise, this leadership responsibility will be assigned as a collateral duty to an Information Security Officer. The RMM is responsible for performing risk management as described in this document and will serve as facilitator for assigned risk analysis groups.

Risk Analysis Group

Project software developers are required to serve as members of risk analysis groups. These groups analyze, document and track risks associated with project development. This group will have from one to five participants. The following criteria should be used in selecting participants.

- a. Knowledge and experience in the technology areas of the effort being assessed.
- b. Assigned to work for the project in the area being assessed.
- c. Contribute to mix of people with various applicable skills (e.g. development, test, quality assurance).
- d. Ensures representation for any functional areas considered critical to the project.

4. Task and Steps

The Risk Management Process in this document applies to all business unit of Ocenture.

Identify Risk

An initial set of risks are presented to the risk management manager. Then the source of the risk(s) are identified and determined if the source is internal or external to the project/enterprise. From this point the risk management manager will identify if the risk is considered short-term or long-term and rather if the risk is executive, strategic, managerial, tactical or operational focused. Note: There are several approaches for dealing with each identified risk: avoidance, assumption, mitigation, and contingency planning.

- a. Avoidance refers to elimination of the risk issue from the project.
- b. Risk assumption means that no action will be taken regarding the risk issue.
- c. Mitigation of risks means that some action is taken between now and the time frame of the risk to moderate the risk exposure - lessen the likelihood of occurrence or the severity of impact.
- d. Contingency planning means that preparations are made, in advance of the risk time frame, to define the action(s) that will be taken should the risk situation occur. In essence, contingency planning is proactive, forward-looking preparation for action for risks that have been assumed and for risks where prior mitigation actions may have been performed.

Risk identification is a continuous process. Therefore, the risk analysis group should meet on a periodic basis to identify new risks and to re-assess current.

Analyze Risk

Each risks analysis group member analyzes the risks identified in order to determine the scope of the risks and if the risks is considered to be on the 'critical path' for continuation of the project. The group member will present his/her findings at the next group meeting.

The group facilitator goes through the project's list of risks, presenting the risks identified and/or changed prior to the meeting and soliciting any other risks from the group. The facilitator presents possible risks to be combined and the group reaches consensus on which are combined.

Prioritize Risk

After consensus has been reached on newly submitted risks, the group facilitator leads a discussion to establish consensus on probability, impact, and impact time frame for each new risk in order to determine risk exposure. These risk exposure(s) are then discussed and analyzed in order to reach a consensus on the ranking and priority for each risk.

Define Avoidance Alternatives

The risk analysis group then performs an analysis to determine if there are any actions or decisions that could be made that would provide avoidance of the risk. One alternative is to change organizational or project processes. This includes strategic and tactical process change authorization by executive decision making staff or project owner.

Define Mitigation Plan for Key Risk

Determine what actions or decisions can be made that reduce the probability and/or severity of impact of key risks. To determine what risks are candidates for the development of a mitigation strategy, the group will analyze the lists of current risks. While all risks should be discussed, risks with medium and high exposure ratings or priorities are serious candidates for development of mitigation strategies.

Define Contingency Plan

For each of the high exposure risks, the group will conduct a session to validate the nature of the event that would call for the development of a contingency plan and/or actions to mitigate the risk. All the high exposure risks will have a mitigation strategy; however, only those risks the risk analysis group deem capable of critically impacting the cost, schedule, or operational suitability are candidates for development of a contingency plan.

Define Risk Metrics

For each risk, determine what measurable or observable event(s) can be tracked to know whether or not the risk is being avoided, prevented, or minimized. Test metrics will include tracking of the difference between open and closed trouble reports and the tracking of error density by trouble report priority.

Implement Mitigation Plan

For each risk with an identified mitigation plan addressed in Step 4.7 above, the project owner will

implement and track that plan. For mitigation plans involving modification of the project's processes, the project owner will initiate the action to update the project's processes. These activities should be documented in each applicable risk's documentation.

Track Risk

The risk analysis group conducts monthly meetings to perform a group analysis of the project's risks. Each member of the risk analysis group analyzes their assigned risks using the current project measurement information to determine the status of each risk. The method and time of collecting and reporting the required metrics should be incorporated into the project's documentation. The designated project owner will ensure the timely reporting of raw data, ensure that derived metrics are computed, and the reporting frequency is as required by the project scope. The project owner will analyze the reports, ensure that the reports are properly filed or archived, and take appropriate corrective actions as required. Note: High exposure risks are marked as candidates for inclusion in the Quarterly Project Review, each being addressed separately as a project risk.

Implement Contingency Plan

For high exposure risks, if the data collected shows that the entrance criteria has been met, then implement the contingency plan for that risk. This action would require raising attention to the need for implementation of a contingency plan to the project owner and allow executive management to provide for the direction necessary to reallocate resources necessary to the execution of that contingency plan.

5. Output

The results of risk analysis are reviewed and the group reaches consensus on the top risks (for example, top 5 risks). The final activity in the risk analysis process is a presentation of the results and a meeting with the project owner, at a minimum. All presentations will be conducted as a formal presentation to all project personnel who are involved in the management of the project on a monthly basis.

Key considerations include having all participants attend and to conduct the presentation such that participants can know what happened to "their" risks and to help determine risks that need to be raised at a Quarterly Project Review with the project owner. An example outline for the presentation appears below.

- a. Review of the risk assessment processes.
- b. Complete lists of risks with attributes.
- c. Top Risk.
- d. Documented contingency events and a summary of each associated plan of action.

6. Exit Criteria

Assessing project risk is a continuous process. As such, the activities defined in Steps 4 are repeated in a cyclic manner until the project has reached a logical conclusion or responsibility has been transferred to another Ocenture business unit.

7. Metrics

Candidate metrics for the Risk Management Process could include, but not be limited to recording the following measurement data associated with risk management activities.

- 7.1. Efforts expended in risk management activities to facilitate an assessment of the cost effectiveness of risk activities.
- 7.2. Each time a risk assessment is performed, record the items listed below.
 - 7.2.1. The date of the risk analysis.
 - 7.2.2. The effort expended on the risk analysis.
 - 7.2.3. The number of risks identified in either: (New Risk or Previous Identified Risk)
 - 7.2.4. The number of previously-identified risks that are no longer considered risks in the following context: (Risk Avoided or Risk that Occurred)

Risk Worksheet

Project Owner: _____ Project Area _____

Date: _____ Office Location: _____ Risk ID: _____

Risk Description:

Probability: _____

Impact: _____

Impact Time Frame: _____ to _____

Critical Path: YES NO

Affected Phase:

Mitigation Plan:

Contingency Plan

Management Change Guidelines

1. Introduction

The Information Resources infrastructure at Ocenture is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong change management process is essential.

From time to time each Information Resource element requires an outage for planned upgrades, maintenance or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance or fine-tuning.

Managing these changes is a critical part of providing a robust and valuable Information Resources infrastructure.

2. Purpose

The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

3. Audience

The Ocenture Change Management Policy applies to all individuals that install, operate or maintain Information Resources.

4. Definitions

Information Resources

Information Resources (IR) any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Owner

The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Custodian

Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For mainframe applications Information Services is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Change Management

The process of controlling modifications to hardware, software, firmware, and documentation to ensure

that Information Resources are protected against improper modification before, during, and after system implementation.

Change

Any implementation of new functionality

Any interruption of service

Any repair of existing functionality

Any removal of existing functionality

Scheduled Change

Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Unscheduled Change

Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure, the discovery of a security vulnerability or there exists a pressing business need as determined by one of the Members of Ocenture, LLC.

Emergency Change

When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.

5. **Change Management Policy**

Every change to an Ocenture Information Resources resource such as: operating systems, computing hardware, networks, and applications is subject to the Change Management Policy and must follow the Change Management Procedures.

All changes affecting computing environmental facilities (e.g., air-conditioning, water, heat, plumbing, electricity, and alarms) need to be reported to or coordinated with the leader of the change management process or by an Officer or Member of the LLC.

A Change Management Committee, appointed by a majority of owners, will meet as needed to review change requests and to ensure that change reviews and communications are being satisfactorily performed.

All scheduled change requests must be submitted in accordance with change management procedures so that the Change Management Committee has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.

Each scheduled change request must receive formal Change Management Committee approval before proceeding with the change.

The appointed leader of the Change Management Committee or any Member of the LLC may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as yearend accounting, or if adequate resources cannot be readily available. Adequate resources may be a problem on weekends, holidays, or during special events.

After launch, Customer notification must be completed for each scheduled or unscheduled change following the steps contained in the Change Management Procedures

A Change Review must be completed for each material change, whether scheduled or unscheduled, and whether successful or not.

A Change Management Log must be maintained for all material changes. The log must contain, but is not limited to:

Date of submission and date of change
Owner and custodian contact information
Nature of Change
Indication of success or failure

All Ocenture information systems must comply with an Information Resources change management process that meets the standards outlined above.

6. **Disciplinary Action**

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of Ocenture's Information Resources access privileges, civil, and criminal prosecution.

7. **Support Information**

The IR network is owned and controlled by Ocenture. Approval must be obtained from IS before connecting a device that does not comply with published guidelines to the network. Ocenture reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secure.

The integrity of general use software, utilities, operating systems, networks, and respective data files are the responsibility of the custodian department. Data for test and research purposes must be de-personalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

8. **Management Change Guidelines References**

Copyright Act of 1976
Foreign Corrupt Practices Act of 1977
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
DIR Practices for Protecting Information Resources Assets
DIR Standards Review and Recommendations Publications

Approvals, Revisions and Adjustments:

Initial Approval

11/01/2006 | 20061101
Fraser Burns, Managing Partner (Approval Code 20061101-216)

Document Updated

01/03/2007 | 20070103
Fraser Burns, Managing Partner (Approval Code 20070103-521)
New design of document to support additions.

Document Updated

01/22/2007 | 20070122
Fraser Burns, Managing Partner (Approval Code 20070122-780)
Updated Access Control Policy

Document Updated

01/22/2007 | 20070122
Fraser Burns, Managing Partner (Approval Code 20070308-329)
Updated Document

Document Updated

03/19/2007 | 20070319
Fraser Burns, Managing Partner (Approval Code 20070319-549)
Information Security Policy

Document Updated

04/02/2007 | 20070402
Fraser Burns, Managing Partner (Approval Code 20070402-620)
Risk Management Processes

Document Updated

04/21/2007 | 20070421
Fraser Burns, Managing Partner (Approval Code 20070421-392)
Change Management Guidelines

I have received and have been briefed on the contents of the Security Policy and Processes of Ocenture, LLC and/or its affiliated companies. I understand I am subjected to the policies and regulations outlined therein, and agree to comply with all standards expected of me. I also acknowledge this manual to be dynamic in nature and subject to review, and/or change at any given time, dependent upon the needs and operational requirements of the company.

Print Name _____

Signature _____ Date _____