

PALM BEACH STATE COLLEGE

ADMINISTRATIVE PROCEDURE

Policy: 6Hx-18-1.XX	Category: Information Technology	Version Date: 0001
Title: Data Classification		Effective Date: 11-01-09
Originating Unit: Information Technology Security Office		Last Review: TBD
Review Officer: Chief Information Officer, Anthony Parziale		Next Review: TBD

Overview:

Employee Responsibility - Every employee who has access to Palm Beach State College information or information systems has an important information security role in the organization. For example, each one of these employees is personally responsible for the protection of information that has been entrusted to their care. All employees who come into contact with sensitive Palm Beach State internal information are expected to familiarize themselves with this data classification policy and to consistently use these same ideas in their daily Palm Beach State business activities. Sensitive information is either Confidential or Secret information, and both are defined later in this document. Although this policy provides overall guidance, to achieve consistent information protection, employees are expected to apply and extend these concepts to fit the needs of day-to-day operations. This document provides a conceptual model for classifying information based on its sensitivity, and an overview of the required approaches to protect information based on these same sensitivity classifications.

Addresses Major Risks - The Palm Beach State data classification system, as defined in this document, is based on the concept of need to know. This term means that information is not disclosed to any person who does not have a legitimate and demonstrable business need to receive the information. This concept, when combined with the policies defined in this document, will protect Palm Beach State information from unauthorized disclosure, use, modification, and deletion.

Consistent Approach Required - A single lapse in information security can have significant long-term consequences. Consistent use of this data classification system is essential if sensitive information is to be adequately protected. Without the consistent use of this data classification system, Palm Beach State unduly risks loss of customer relationships, loss of public confidence, internal operational disruption, excessive costs, and competitive disadvantage. This policy consistently protects sensitive information no matter what form it takes, what technology is used to process it, who handles it, where the information may be located, and in what stage of its life cycle the information may be.

Data Classification Policy

Purpose:

The purpose of this policy is to establish a standard for classifying Palm Beach State data, the protection of those passwords and the frequency of change.

Scope:

This data classification policy is applicable to all information in the possession or under the control of Palm Beach State. For example, confidential information entrusted to Palm Beach State by customers, business partners, suppliers, and other third parties must be protected with this data classification policy. Employees are expected to protect third-party information with the same care that they protect Palm Beach State information. No distinctions between the words "data," "information," "knowledge," and "wisdom" are made for purposes of this policy.

Guidelines:

Access Control

Need to Know - Every one of the policy requirements set forth in this document are based on the concept of need to know. If an employee is unclear how the requirements set forth in this policy should be applied to any particular circumstance, he or she must conservatively apply the need to know concept. That is to say that information must be disclosed only to those people who have a legitimate business need for the information. This principle applies to private employee information such as medical histories, just as it applies to proprietary College information such as plans for a new product.

System Access Controls - Access to all Palm Beach State sensitive computer-resident information must be protected by access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. Traditional access control systems employ user IDs and fixed passwords, but these are currently being phased out in favor of more secure technologies such as dynamic passwords and biometrics. Whatever technology is employed, access must be controlled for each individual based on that individual's need to know. The notion of the need to know includes not only viewing information, but other privileges such as modifying information or using information to complete a transaction. Palm Beach State access control systems must log which users accessed what sensitive data, and the time and date of each such access.

Access Granting Decisions - Access to Palm Beach State sensitive information must be provided only after the written authorization of the information Owner has been obtained. Custodians of the involved information must refer all requests for access to the relevant Owners or their delegates. Standard templates of system privileges are defined

for all job titles, and Owners approve these privileges in advance. Special needs for other access privileges will be dealt with on a request-by-request basis.

Classification Labels

Owners And Production Information - All production information types possessed by or used by a particular organizational unit within Palm Beach State must have a designated Owner. Production information is information routinely used to accomplish business objectives. Examples include payroll summaries, shipping schedules, and managerial cost accounting reports. Information Owners are responsible for assigning appropriate sensitivity classifications as defined below. Owners do not legally own the information entrusted to their care. They are instead designated members of the Palm Beach State management team who act as stewards, and who supervise the ways in which certain types of information are used and protected.

SECRET - This classification label applies to the most sensitive business information that is intended for use strictly within Palm Beach State. Its unauthorized disclosure could seriously and adversely impact Palm Beach State, its customers, its business partners, and its suppliers. Examples include merger and acquisition documents, College level strategic plans, litigation strategy memos, reports on breakthrough new product research, and Trade Secrets such as certain computer programs.

CONFIDENTIAL - This classification label applies to less-sensitive business information that is intended for use within Palm Beach State. Its unauthorized disclosure could adversely impact Palm Beach State or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally-generated market research, computer passwords, identity token personal identification numbers, and internal audit reports.

FOR INTERNAL USE ONLY - This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact Palm Beach State or its employees, suppliers, business partners, or its customers. Examples include the Palm Beach State telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.

PUBLIC - This classification applies to information that has been approved by Palm Beach State management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

Other Labels - Palm Beach State department or division-specific data classification labels are permissible, but must be consistent with and supplemental to the Palm Beach State data classification system. These supplementary labels might for example include the use of words like "Private" or "Financial."

Owners And Access Decisions - Owners must make decisions about who will be permitted to gain access to information, and the uses to which this information will be put. Owners must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information. Readers of this policy can quickly determine the appropriate Owner by consulting the Information Technology Security Office's (ITSO) page on the Palm Beach State intranet.

Labeling

Consistent Classification Labeling - If information is sensitive, from the time it is created until the time it is destroyed or declassified, it must be labeled with an appropriate data classification designation. Such markings must appear on all manifestations of the information, such as hard copies, floppy disks, and CD-ROMs. Employees must not remove or change data classification system labels for sensitive information unless the permission of the Owner has been obtained.

What Gets Labeled - The vast majority of Palm Beach State information falls into the Internal Use Only category. For this reason, it is not necessary to apply a label to Internal Use Only information. Information without a label is by default classified as Internal Use Only.

Labels Believed To Be Incorrect - If the recipient of Palm Beach State internal information believes that the data classification label accompanying this information is incorrect, the recipient must protect the information in a manner consistent with the more stringent of the two possible classification labels. Before using this information or distributing it to any other party, such a recipient must check with the information Owner to ensure that the label currently applied to the information is correct.

Information Collections - Employees who create or update a collection of information are responsible for choosing an appropriate data classification label for the new collection. This label must be consistent with the decisions made by the relevant Owners and generally should be the most restricted classification level found in the collection. For example, if a new database is being created, and if it contains Internal Use Only and Confidential information, then the entire database must be classified as Confidential. Other examples of such collections include an internally-generated competitive intelligence report, management decision background reports, and access-controlled intranet pages. At the time that it is being compiled, every employee creating a new

Data Classification Policy

collection of this nature must notify the involved information Owner about the creation of their new collection.

Storage Media - If information recorded on computer storage media with a higher sensitivity classification is moved to media with a lower sensitivity classification, then the media with the lower sensitivity classification must be upgraded so that its classification reflects the highest sensitivity classification. For example, if information labeled Secret were to be placed on a floppy disk containing information with no label, then the floppy disk must immediately be reclassified as Secret. If information with several different data classification levels is resident on a single computer, then the system controls must reflect the requirements associated with most restrictive data classification level. In general, because it increases handling costs and operational complexity, commingling information with different sensitivity classifications is discouraged.

Labels For Externally-Supplied Information - With the exception of general business correspondence and copyrighted software, all externally-provided information that is not clearly in the public domain must receive a Palm Beach State data classification system label. The Palm Beach State employee who receives this information is responsible for assigning an appropriate classification on behalf of the external party. When assigning a Palm Beach State classification label, this staff member must preserve copyright notices, author credits, guidelines for interpretation, and information about restricted dissemination.

Labeling Hardcopy - All printed, handwritten, or other paper manifestations of sensitive information must have a clearly-evident sensitivity label on the upper right hand corner of each page. If bound, all paper manifestations of sensitive information must have an appropriate sensitivity label on the front cover, the title page, and the rear cover. The cover sheet for faxes containing sensitive information must contain the appropriate classification label. Microfiche and microfilm also must contain labels if they contain sensitive information.

Labeling Computer Storage Media - All CD-ROMs, floppy disks, and other computer storage media containing sensitive information must be externally labeled with the appropriate sensitivity classification. Unless it would adversely affect the operation of an application program, computer files containing sensitive information must also clearly indicate the relevant classification label in the first two data lines.

Other Displays - If information is sensitive, all instances in which it is displayed on a screen or otherwise presented to a computer user must involve an indication of the information's sensitivity classification. Teleconferences and telephone conference calls where sensitive information will be discussed must be preceded by a statement about the sensitivity of the information involved. Teleconferences and telephone calls where

Data Classification Policy

sensitive information is discussed must be preceded by a determination that all parties to the discussion are authorized to receive the sensitive information. Persons other than those specifically invited must not attend meetings where sensitive information will be discussed.

Additional Public Information Labels - Unless it is unquestionably already public information, all Palm Beach State information with a Public label must also be labeled "Approved For Public Release" along with the date when the Owner declared the information Public.

Dictation Devices And Tape Recorders - To reduce the chance of unauthorized disclosure, in general, employees must not record sensitive information with dictation devices, tape recorders, telephone answering machines, or similar devices. If the use of these devices is an operational necessity, the proper sensitivity classification must be specified at the beginning and end of each segment of sensitive information. In this case, the recording media must also be marked with the most stringent data classification found on the media. In addition, the media must be protected in accordance with the most stringent classification found on the media, and erased as soon as possible.

Third-Party Interactions

Third Parties And The Need To Know - Unless it has been specifically designated as Public, all Palm Beach State internal information must be protected from disclosure to third parties. Third parties may be given access to Palm Beach State internal information only when a demonstrable need to know exists, and when such a disclosure has been expressly authorized by the relevant Palm Beach State information Owner. Contractors, consultants, temporaries, volunteers and every other type of individual or entity that is not a Palm Beach State employee, is by definition a third party for purposes of this policy.

Disclosures To Third Parties And Non-Disclosure Agreements - The disclosure of sensitive information to consultants, contractors, temporaries, or any other third parties must be preceded by the receipt of a signed Palm Beach State non-disclosure agreement. Disclosures of Palm Beach State sensitive information to these third parties must be accompanied by a running log indicating exactly what type of information was provided. This log will be important when the time arrives to recover these materials or obtain a letter certifying destruction of the materials at the end of a contract.

Disclosures From Third Parties And Non-Disclosure Agreements - Employees must not sign non-disclosure agreements provided by third parties without the authorization of Palm Beach State legal counsel designated to handle intellectual property matters. These forms may contain terms and conditions that unduly restrict the future business directions of Palm Beach State.

Third-Party Requests For Palm Beach State Information - Unless an employee has been authorized by the information Owner to make public disclosures, all requests for information about Palm Beach State and its business must be referred to Public Relations. Such requests include questionnaires, surveys, and newspaper interviews. This policy does not apply to sales and marketing information about Palm Beach State products and services, nor does it pertain to customer support calls.

Prior Review - Every speech, presentation, technical paper, book, or other communication to be delivered to the public must have been approved for release by the involved employee's immediate manager. This policy applies if the employee will represent Palm Beach State or discuss Palm Beach State affairs, or if the communication is based on information obtained in the course of performing Palm Beach State job duties. If new products, research results, College strategies, customer information, or marketing approaches are to be divulged, prior approval of the director of Research and Development and the director of the Legal department also must be obtained.

Owner Notification - If sensitive information is lost, is disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information Owner and the manager of the ITSO must be notified immediately.

Shipping And Handling

Making Copies - Making additional photocopies or printing extra copies of sensitive information must not take place without the advance permission of the information Owner. Employees must be aware that selected Palm Beach State photocopy machines and fax machines keep logs of the information copied or faxed.

Unattended Printing - Printers must not be left unattended if sensitive information is being printed or soon will be printed. The persons attending the printer must be authorized to examine the printed information. Unattended printing of sensitive information is permitted only if physical access controls are used to prevent unauthorized persons from entering the area by the printer and viewing the material being printed.

Use Of Outside Services - Prior to sending any sensitive information to a third party for copying, printing, formatting, or other handling, the third party must sign a Palm Beach State non-disclosure agreement.

Page Numbering - All sensitive Palm Beach State information manifested in paper form must indicate both the current and the last page, for example, "Page X of Y."

Data Classification Policy

Backup Storage Media - All sensitive information recorded on backup computer media and stored outside Palm Beach State offices must be in encrypted form. If an encryption system with key escrow is not used for this purpose, all keys used to make these backup copies must be promptly provided to the ITSO shortly after their initial use.

Envelopes - If sensitive information is to be sent through internal mail, external mail, or by courier, it must be enclosed in two envelopes or containers. The outside envelope or container must not indicate the classification or the nature of the information contained therein. The inside sealed and opaque envelope or container must be labeled with the appropriate classification label. Envelopes containing sensitive information must be addressed to a specific person, and must contain sufficient return address information. All sensitive Palm Beach State information sent through these delivery systems must require a signature by an authorized party at the destination.

Delivery Of Computer Output - Sensitive computer system output must be personally delivered to the designated recipients. Such output must not be delivered to an unattended desk, placed in an uncontrolled computer output receptacle, or left out in the open in an unoccupied office. It may be made available to only the designated recipients through password-protected fax mailboxes, departmental or personal computer output lockers, or other physical security methods.

Removal From Offices - Sensitive Palm Beach State information must not be removed from Palm Beach State premises unless there has been prior approval from the information's Owner. This policy includes portable computers with hard disks, floppy disks, hard-copy output, and paper memos. An exception is made for authorized offsite backups.

Locked Containers In The Office - Sensitive information in hardcopy form must be secured when not actively in use, even if it is within a building to which access is controlled. If not encrypted, all sensitive information must be locked in safes, heavy furniture, or other containers approved by the ITSO. Unattended sensitive information found lying on a desk after business hours, or sensitive information that is otherwise readily accessible to passers-by after hours, may be confiscated and later claimed in person from the ITSO.

Locked Containers Off-Site - Whenever a hardcopy version of sensitive information is removed from Palm Beach State premises, it must be carried in a locked briefcase or container when not in use. Such information must not be left in an unattended motor vehicle, hotel room, office, or some other location, even if the vehicle or room is locked.

Oral Warnings - If Confidential information is released orally in a meeting, seminar, lecture, or related presentation, the speaker must communicate the sensitivity of the information. The speaker must remind the audience to use discretion when disclosing it

to others. Visual aids such as projector slides and overhead transparencies must include the appropriate data classification labels.

Cellular And Cordless Phones - Unless an encrypted link has been established, employees must never discuss sensitive information over cellular or cordless phones. For the same reason, radio local area networks must not be used to transmit sensitive information unless an encryption process approved by the ITSO is consistently employed. Computer links established over cellular phones or other airwave broadcast systems must not include the transfer of sensitive information unless the link is known to be encrypted. Internet telephone facilities must not be employed to discuss sensitive Palm Beach State information unless the link is encrypted.

Declassification And Downgrading

Dates For Reclassification - If known, the date that Secret or Confidential information will no longer be sensitive or declassified must be indicated on all Palm Beach State sensitive information. This will assist those in possession of the information with its proper handling, even if these people have not been in recent communication with the information's Owner. Those employees in possession of sensitive information that was slated to be declassified on a date that has come and gone, but is not known definitively to have been declassified, must check with the information Owner before they disclose the information to any third parties.

Classification Extensions - The designated information Owner may, at any time prior to scheduled declassification or downgrading, extend the period that information is to remain at its current classification level. To achieve this, the Owner must change the declassification or downgrading date appearing on the original document, notify all known recipients and Custodians, initiate a cost-effective search for additional recipients, and notify the Palm Beach State archives Custodian. Owners must not to specify a date for declassification or downgrading unless they are relatively sure that the date will not be changed.

Notifications - The designated information Owner may, at any time, declassify or downgrade the classification of information entrusted to his or her care. To achieve this, the Owner must change the classification label appearing on the original document, notify all known recipients and Custodians, and notify the Palm Beach State archives Custodian.

Schedule For Review - To determine whether sensitive information may be declassified or downgraded, at least once annually, information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical. Owners must follow the guidelines for declassification and downgrading as

specified in the information ownership policy.

No Unauthorized Downgrading - Employees must not move information classified at a certain sensitivity level to a less sensitive level unless this action is a formal part of a declassification or downgrading process approved by the Owner.

Destruction And Disposal

Destruction And Disposal - All Palm Beach State information must be destroyed or disposed of when no longer needed for business purposes. To support this policy, information Owners must review the continued value and usefulness of information on a periodic basis. Owners also must review the data retention schedule issued by the Legal department to determine the minimum legal periods that information must be retained.

Destruction And Locked Boxes - All sensitive information no longer being used or no longer needed must be placed in designated locked metal boxes until such time as authorized Palm Beach State personnel or a bonded destruction service picks it up. If no locked disposal boxes are in the immediate vicinity, sensitive information in hardcopy form must be either shredded or incinerated, while sensitive information in all other forms must be delivered to the Physical Security department for secure destruction. The shredders used for this purpose must create confetti or other similar small particles. Strip-cut shredders must not be used for this purpose. Erasing or reformatting magnetic media such as floppy disks is not an acceptable data destruction method. The use of overwriting programs approved by the ITSO is permissible as a way to destroy sensitive information on magnetic storage media such as floppy disks. Only after these programs have been used can storage media containing sensitive information be reused, trashed, recycled, or donated to charity.

Destruction Approval - Employees must not destroy or dispose of potentially important Palm Beach State records or information without specific advance management approval. Unauthorized destruction or disposal of Palm Beach State records or information will subject the employee to disciplinary action including termination and prosecution. Records and information must be retained if they are likely to be needed in the future, regulation or statute requires their retention, or they are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts. Any questions about data destruction must be referred to the information Owner or the Owner's delegate.

Permissible Destruction - Employees may destroy Palm Beach State records when approval has been granted by verbal instructions from the Owner or the Owner's delegate, an ITSO or Archive department memo detailing the type of records that may be destroyed and when, or the records retention and disposition schedule issued by the

Data Classification Policy

Legal department. Destruction is defined as any action that prevents the recovery of information from the storage medium on which it is recorded.

Intermediate Products - All materials used in the handling of sensitive information, which could be analyzed to deduce sensitive information, must be destroyed in a manner similar to that required for sensitive information. This policy covers typewriter ribbons, carbon paper sheets, mimeograph stencil masters, photographic negatives, aborted computer hardcopy output, and unacceptable photocopies.

Photocopies - All waste copies of Secret information that are generated in the course of copying, printing, or other sensitive information handling must be destroyed according to the instructions found in this policy. If a copy machine jams or malfunctions when employees are making copies of Secret information, the involved employees must not leave the machine until all copies of the information are removed from the machine or destroyed beyond recognition.

Equipment Disposal Or Servicing - Before computer or communications equipment is sent to a vendor for trade, servicing, or disposal, all Palm Beach State sensitive information must be destroyed or concealed according to methods approved by the ITSO. Internal hard drives and other computer storage media may not be donated to charity, disposed of in the trash, or otherwise recycled unless they have been subjected to overwriting processes approved by the ITSO.

Physical Security

Office Access - Access to every office, computer room, and work area containing sensitive information must be physically restricted. Management responsible for the staff working in these areas must consult the Physical Security department to determine the appropriate access control method.

Locked When Not In Use - When not in use, sensitive information must be protected from unauthorized disclosure. When left in an unattended room, such information must be locked in appropriate containers. If a Custodian of such information believes he or she will be away for less than 30 minutes, the information may be left on a desk or in some other readily-observed spot only if all doors and windows to the unattended room are closed and locked.

Unauthorized Screen Viewing - The screens on computers used to handle sensitive information must be positioned such that unauthorized persons cannot readily look over the shoulder of the person using the workstation. Screens should be positioned such that sensitive information cannot be seen through windows or skylights using binoculars or telescopes.

Special Considerations For Secret Information

Background Checks - All employees who will have access to Secret information must have passed a standardized background check performed by the Human Resources department. Access to Secret information must not be provided before this background check is completed.

Storage On Personal Computers - If Secret information is going to be stored on a personal computer, portable computer, personal digital assistant, or any other single-user system, the system must support and continuously run an access control package approved by the ITSO. When these users are not currently accessing or otherwise actively using the Secret information on such a machine, they must not leave the machine without logging off, invoking a screen saver, or otherwise restricting access to the Secret information.

Numbering Document Copies - All copies of Secret documents must be individually numbered with a sequence number to ensure that the persons responsible for the documents and the location of the documents can both be readily tracked. Hardcopy manifestations of Secret information must include the words "Do Not Copy Without Explicit Permission From The Information Owner."

Secret Information Logs - When Secret information is involved, the Owner or delegate of the Owner must keep a log reflecting the number of copies made, the location of copies, the names of recipients, the addresses of recipients, and any persons viewing the copies. This log must be maintained as long as such information retains a Secret sensitivity classification. This log also must be classified as Secret. All production application systems that handle Secret Palm Beach State information must generate logs that show every addition, modification, and deletion to such Secret information.

Removal From Offices - Secret Palm Beach State information must not leave Palm Beach State offices unless the approval of the Information Security manager has been obtained.

Couriers - Secret information in hardcopy form must be sent by trusted courier or registered mail. Other methods such as regular mail are prohibited. All deliveries of Secret information must be conducted such that the intended recipient personally acknowledges that the information has been received. Delivery of secret information to intermediaries such as receptionists is prohibited.

Transportation With Computers - Employees in the possession of portable, laptop, notebook, handheld, personal digital assistant, and other transportable computers containing Secret Palm Beach State information must not leave these computers unattended at any time unless the Secret information has been encrypted. If Secret data is to be transported in computer-readable storage media, it must be in encrypted form.

Data Classification Policy

Viewing In Public - Employees must avoid traveling on public transportation when in the possession of Secret information. Secret information must not be read, discussed, or otherwise exposed on airplanes, or in restaurants, elevators, restrooms, or other public places. Palm Beach State employees must not take Secret Palm Beach State information into another country unless permission has been obtained from the Physical Security manager.

Storage - Computerized Secret information must be encrypted when not in active use. All systems used for the processing of Secret information must be powered down immediately after processing is completed, or have these temporary storage locations overwritten with programs approved by the ITSO.

Transmission Over Networks - If Palm Beach State Secret data is to be transmitted over any communication network, it must be sent only in encrypted form. Such networks include internal electronic mail systems, the Internet, and dial-up lines. All such transmissions must use a virtual public network or similar software as approved by the ITSO.

Transfer To Another Computer - Before any Secret information may be transferred from one computer to another, the person making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer. If comparable security cannot be provided with the destination system's access controls, then the information must not be transferred.

Fax Transmission - Secret information must not be sent to an unattended fax machine unless the destination machine is in a locked room for which only people authorized to receive the information possess the keys. Transmission to a fax server that uses passwords to control access to received faxes is a permissible exception to this policy. All fax transmissions containing Secret data must also employ an encrypted link.

Speaker Phones - Secret information must not be discussed on speakerphones unless all participating parties acknowledge that no unauthorized persons are in close proximity such that they might overhear the conversation. Employees must refrain from leaving messages containing Secret information on answering machines or voice mail systems.

Telephone Conversations - Employees must take steps to avoid discussing sensitive information when on the telephone. If discussion of such information is absolutely required, employees must use guarded terms and refrain from mentioning sensitive details beyond those needed to get the job done.

Data Classification Policy

Enforcement:

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

Contact Information:

Questions, concerns or comments concerning this guideline should be directed to:

Tony Parziale

CIO

Palm Beach State College

4200 Congress Avenue, ITB 103

Lake Worth, Florida 33461

Tel: 561.868.3262

Fax: 561.868.3259

Revision History:

Version	Revision Date	Review Date	Description
1.0	06/30/2009		