1. Introduction
This Information Assurance (IA) Security Plan describes Bellevue University's safeguards to protect covered data and information (hereafter referred to as covered information) and the computer systems on which it resides. The Plan documents the framework for the protection of the confidentiality, integrity, availability, and accountability of covered information. In addition to this Plan, other University policies on data confidentiality and safeguarding may apply to specific data, computers, computer systems, or networks provided or operated by University departments.

2. Applicability
This Plan derives its authority from specific University policies, and therefore applies to everyone who uses, maintains or manages University business processes which involve covered information. The Plan applies wherever covered information is located, whether on campus or from remote locations or whether it's in paper or electronic form. The Plan will be evaluated periodically and adjusted as necessary in light of relevant circumstances.

3. Responsibilities
The University has appointed the Director of Application Development and the Director of Infrastructure Operations as Co-Information Systems Security Officers (ISSO) to act as the co-coordinators of this Plan. These positions are responsible for assessing the risks associated with protecting covered information and implementing procedures to minimize those risks to Bellevue University. These positions are also responsible for verifying that violators of this plan are reported to individual supervisors for corrective actions. Appendix 1 contains the letter declaring the current positions and employees assigned as ISSO. Appendix 2 contains the job descriptions for these positions.

4. Covered Information
Covered information for the purpose of this plan includes, but is not limited to University employees' and students' personal and financial information required to be protected under federal or state law. Student financial information is that information that Bellevue University has obtained from a customer in the process of offering a financial product or service, or such information
provided to the University by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format. Personal information is any data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Bellevue University is obligated to comply with certain educational records standards pursuant to the Family Educational Rights and Privacy Act ("FERPA"). To the extent applicable, FERPA, as well as Bellevue University’s FERPA compliance policy, govern the collection and use of information. Additional information on FERPA is found here: [http://www.bellevue.edu/about/consumer-information/ferpa-information.aspx](http://www.bellevue.edu/about/consumer-information/ferpa-information.aspx).

5. Identification and Assessment of Risk to Covered Information

Bellevue University recognizes that it has both internal and external risks associated with protecting covered information. These risks include, but are not limited to:

- Unauthorized access of covered information by someone other than the owner of the covered information;
- Compromised system security as a result of system access by an unauthorized person;
- Interception of data during transmission;
- Loss of data integrity;
- Physical loss of data in a disaster;
- Errors introduced into the system;
- Corruption of data or systems;
- Unauthorized access of covered information by employees;
- Unauthorized requests for covered information;
- Unauthorized access through hardcopy files or reports; and
- Unauthorized transfer of covered information through third parties.
Bellevue University recognizes that this is not a complete list of the risks associated with the protection of covered information. Since technology growth is dynamic, new risks are regularly created.

6. Design and Implementation of Safeguards Program

A. Security Policies
The University has established and will maintain Information security policies to ensure the appropriate handling and protection of covered information and the IT systems on which it resides. Relevant Information Security policies include:

- Policy Statement 445, Information Security
- Policy Statement 450, Operational Network and Physical Security
- Policy Statement 402, Computer and Network Use
- Policy Statement 401, Management and Use of E-Mail
- Policy Statement 2400, Security and Control of Student Permanent Records
- Policy Statement 13, Student Records Policies and Procedures

In support of these policies, Information Security requirements and regulations for students are also published in the Bellevue University Catalog and Bellevue University Student Handbook.

B. Employee Management and Training
All new employees receive orientation on information security policies. As a condition of being assigned access authorization to the University systems, the user is required to sign an Information Security Acknowledgement Form. This record will be kept in the authorized user’s permanent Human Resources (HR) file (reference PS 445).

New employees are required to certify that they have read and will comply with the Bellevue University Employee Handbook (and Information Security policies referenced within) which includes the use of IT systems, social media, software use, etc. and recertify as updates to the handbook are made.

New employees regularly in contact with covered information are expected to take appropriate steps to protect it (Reference PS 2400 and PS 13). All employees are subject to reference and background checks, including those working in areas that have regular access to covered information (Cashier's Office, Registrar, and Student Financial Assistance). During employee
orientation, each new employee in these departments receives training on the importance of confidentiality of student records, student financial information, and other types of covered information.

C. Physical Security
In accordance with PS 450, Bellevue University Computer Services staff and University employees have the responsibility for ensuring the security of the physical and electronic network and information systems components (both academic and administrative) to a reasonable and economically feasible degree against fraudulent activities and unauthorized access to private information stored within these systems. Access to the University's Controlled Network Areas is restricted to authorized personnel only.

D. Securing Information Systems
In accordance with PS 445, Bellevue University and University employees have the responsibility for securing the information contained within the enterprise systems (both academic and administrative) to a reasonable and economically feasible degree against fraudulent activities and unauthorized access to private information stored within these systems. This responsibility includes maintaining strong user passwords, careful use and management of personal information about students, and the appropriate disposal of confidential information once the business need for the information has been completed.

Bellevue University's data network is a "Private Network" and, as such, is restricted to use by employees, faculty, students, alumni, and those others specifically authorized its use (reference PS 402). Bellevue University authorizes user accounts solely for use in conducting course related research and University business. Any person using the computer or network resources does so within the bounds of this authorization (reference Student Handbook, Computer and Network Use).

Access to covered information via the University's computer information system is limited to those employees who have a business reason to know such information. Databases containing covered information, including, but not limited to, accounts, balances, and transactional information, are available only to University employees in appropriate departments and positions.
Key points of these restrictions are contained in the Bellevue University Security Notice which is displayed as a banner when users begin the system login process. The notice contains statements identifying that it is a private network, used for authorized purposes, by authorized individuals, and it cautions that unauthorized use may result in prosecution. It identifies that the data on the network is owned by Bellevue University and that users consent to monitoring. All users must accept the conditions set forth in the banner prior to accessing the network.

Bellevue University takes reasonable and appropriate steps consistent with current technological developments to ensure the University IT systems and covered information are secure, and to safeguard the integrity of records in storage and transmission. These actions include but are not limited to the following:

- Maintaining the system configuration (reference PS 402 and 445), including the application of appropriate patches and updates.
- Requiring user account passwords to comply with the Bellevue University Policy (reference PS 445).
- Limiting connectivity to only authorized computing equipment (reference PS 445).
- Limiting use of IT systems to student research and university business (reference PS 402 and 445).
- Conducting periodic PC audits to ensure compliance with software licensing regulations (reference PS 402).
- Defining appropriate use of the IT systems and response to violations (reference PS 402).

E. Incident Response
The University has designated members of an Incident Response Team (IRT) who are responsible for responding to actual or attempted security incidents or issues (reference PS 445).

F. Protecting against Malicious Software
Laptop and desktop computers provided to University users shall have University standard anti-virus software installed to protect against malicious software. This software is designed to be automatically updated whenever updates are made available by the manufacturer. All Users are
required to immediately accept any updates that are applied to their machine through the anti-
virus software update programs (reference PS 445).

G. Violations
All users who are suspected of violating the Computer and Network Use Policy will lose their
access privileges to Bellevue University's computing systems pending an evaluation of the
alleged violations (reference BU Catalog and PS 402). Employee violations of Computer and
Network Use Policy will be investigated and appropriate corrective action may be taken up to
and including termination of employment (reference PS 402).

Bellevue University believes the foregoing information technology safeguards are reasonable for
covered information as defined above.

7. Selection of Appropriate Service Providers
Due to the specialized expertise needed to design, implement, and service new technologies,
vendors may be needed to provide resources that the University determines not to provide on its
own. In the process of choosing a service provider that will maintain or access covered information,
the evaluation process shall include the ability of the service provider to appropriately safeguard
covered information in accordance with Bellevue University Policies.

8. Continuing Evaluation and Adjustment
This Information Security Plan is subject to periodic review and adjustment. Continued
administration of the development, implementation and maintenance of the program will be the
responsibility of the Bellevue University Information Systems Security Officers who will assign
specific responsibility as appropriate.

9. Questions
Questions regarding this plan should be sent to the Bellevue University Information Systems
Security Officers.
Appendix 1 – ISSO Designation Letter

July 23, 2014

James Verebely, Assistant Vice President, Information Technology Services
Edward Jarecki, Assistant Vice President, PMO & Enterprise Applications

Re: Assignment as Co-Information Systems Officers (ISSO)

Dear Sirs:

This letter designates the following positions as Co-Information Systems Security Officers (ISSO). The designation formalizes responsibilities that are currently being carried out by the incumbents.

1. Director of Application Development
2. Director of Infrastructure Operations

The two positions will be responsible for working together to:

1. Assess the risks with protecting covered information as defined in the Bellevue University Information Assurance Security Plan
2. Implement procedures necessary to minimize risks to covered information
3. Verify the University departments comply with the requirements of the plan and that violators are reported to individual supervisors for corrective actions, as appropriate.
4. Implement the applicable provisions in the following existing university policy statements and any subsequent updates or new policies that are applicable:
   a. PS 445, INFORMATION SECURITY
   b. PS 402, COMPUTER AND NETWORK USE
   c. PS 450, OPERATIONAL NETWORK AND PHYSICAL SECURITY
   d. PS 618, PASSWORD
5. Establish the process to regularly review and update the Bellevue University Information Assurance Security Plan.

Martyne M. Hallgren
Vice President, Enterprise Services

cc: John Calabrese, Director of Infrastructure Operations
    Doug Eipperle, Director of Application Development
    Lori Iossi, Senior Director of Human Resources

Appendix 2 - ISSO Position Descriptions

Position Title: Director of Infrastructure Operations
Status: Full-time
Classification: Exempt
Reporting Supervisor Title: AVP Information Technology
Work Area/Department: Information Technology Services (ITS)

Primary Function: The Director of Infrastructure Operations role is to plan, organize, and manage staff and overall operations to ensure the stable operation of the organization’s IT infrastructure. This includes developing, maintaining, supporting, and optimizing key functional areas, particularly network infrastructure, server infrastructure, data communications, and telecommunications systems. The Director of Infrastructure Operations will also schedule and direct activities to resolve hardware and software problems in a timely and accurate fashion. The position also serves as an Information System Security Officer to ensure university information is protected.

Duties and Responsibilities:
- Design and implement short- and long-term strategic plans to ensure infrastructure capacity meets existing and future requirements.
- Develop, implement, and maintain policies, procedures, and associated training plans for infrastructure administration.
- Participate in the development of IT strategies in collaboration with the executive team.
- Conduct research and make recommendations on products, services, protocols, and standards in support of all infrastructure procurement and development efforts.
- Establish service level agreements with business units.
- Practice network asset management, including maintenance of network component inventory and related documentation.
- Develop maintenance schedules for network and systems equipment.
- Conduct system feasibility studies and testing.
- Prepare RFPs, bid proposals, contracts, scope of work reports, and other documentation for infrastructure projects and associated efforts.
- Negotiate with vendors, outsourcers, and contractors to secure infrastructure-specific products and services.
- Assist with the planning and deployment of infrastructure security measures.
- Conduct research and remain current with the latest technologies and solutions in support of procurement efforts.
- Manage and set priorities for the design, maintenance, development, and evaluation of all infrastructure systems, including LANs, WANs, Internet, intranet, security, wireless implementations, and so on.
- Conduct feasibility studies for various upgrade projects, improvements, and other conversions.
- Define hardware and software standards in conjunction with owners and stakeholders.
- Test network performance and provide network performance statistics and reports; develop strategies for maintaining network infrastructure.
- Test server performance and provide network performance statistics and reports; develop strategies for maintaining server infrastructure.
• Manage operational costs; conduct near- and long-term financial forecasts for expanded functionality/user base.
• Manage and ensure effectiveness of servers, including e-mail, print, and backup servers, and their associated operating systems and software.
• Manage and ensure optimal operation of all network hardware and equipment, including routers, switches, hubs, UPSs, and so on.
• Manage and ensure effectiveness of security solutions, including firewalls, anti-virus solutions, and intrusion detection systems.
• Establish and maintain regular written and in-person communications with the organization’s executives, decision-makers, stakeholders, department heads, and end users regarding pertinent infrastructure activities.
• Practice IT asset management, including maintenance of component inventory and related documentation.
• Assess and develops strategies to mitigate risk to securing protected information.
• Ensure departments comply with established information security procedures.
• Review and update the information assurance security plan.
• Supervises and develops assigned personnel
  ➢ Responsible for hiring and training new staff.
  ➢ Provides staff with clear directions and priorities that emphasize quality standards, service, morale building, and teamwork.
  ➢ Sets specific goals for staff that align with the strategic business objectives.
  ➢ Monitors and reviews performance of assigned personnel on a continuous (weekly, monthly, quarterly and yearly) basis.
  ➢ Develops and coaches assigned personnel to systematically assure the highest quality service.
  ➢ Advises staff members in resolving problems and issues that arise with internal and external customers.

Qualifications/Skills:
• Bachelor’s degree in the field of computer science, business administration or related discipline required.
• Eight (8) years experience managing and delivering infrastructure design and operational excellence.
• Advanced knowledge of service and application delivery, as well as successful service level agreement accomplishments.
• Advanced technical knowledge of network and PC operating systems
• Hands-on experience troubleshooting hardware such as servers, routers, bridges, switches, hubs, modems, network interface cards, and so on.
• Advanced knowledge of current protocols and standards.
• Conversant with programming languages.
• Experience in interpreting the applicability of local and federal laws/regulations to company operations.
• Demonstrated leadership and personnel/project management skills.
• Strong interpersonal, written, and oral communication skills.
• Ability to perform general mathematical calculations for the purpose of creating needs assessments and budgets.
• Ability to conduct research into issues and products as required.
- Ability to prioritize and execute tasks in a high-pressure environment and make sound decisions in emergency situations.
- Ability to present ideas in a user-friendly language.
- Highly self-motivated and directed.
- Ability to identify complex problems and reviewing related information to develop and evaluate options and implement solutions that address root cause issues.
- Strong customer service orientation.
- Experience working in a team-oriented, collaborative environment.

**Position Title:** Director of Application Development

**Status:** Full-time, Regular

**Classification:** Exempt

**Reporting Supervisor Title:** AVP Information Technology

**Work Area/Department:** Information Technology Services (ITS)

**Primary Function:**

**Application Development & Configuration:** The Director of Application Development is responsible for the leadership, planning, coordinating, and supervision of all activities related to the design, development, and implementation of organizational information systems and software applications. This position will be responsible for providing input on the strategic planning and budgeting. The Senior Director operates independently under broadly defined objectives and manages a department of developers and analysts who support maintenance and improvement of the university’s Oracle PeopleSoft ERP and other core systems. This Senior Director is also responsible for maintaining, supporting, and upgrading existing systems and applications. This individual will apply proven communication skills, problem-solving skills, and knowledge of best practices to guide his/her team on issues related to the design, development, and deployment of mission-critical information and software systems.

**IT Security:** Responsible for establishing and maintaining the information technology risk and security management to ensure that business information and technology assets are adequately protected. Also responsible for identifying, evaluating and reporting on information security risks in a manner that meets compliance and regulatory requirements, and aligns with and supports the risk posture of the enterprise.

**Duties and Responsibilities:**
- Manage the development and deployment of new applications, systems software, interfaces, and/or enhancements to existing applications throughout the enterprise.
- Research and make recommendations on software products and services in support of procurement and development efforts.
- Lead the definition and design phases of development by evaluating proposals in order to identify potential problem areas, and make the appropriate recommendations.
- Ensure that development projects meet business requirements and goals, fulfill end-user requirements, and identify and resolve systems issues.
• Review and analyze existing application effectiveness and efficiency, and develop strategies for improving or leveraging these systems.
• Cultivate, disseminate, and enforce functional policies, procedures, and quality assurance best practices.
• Manage aspects of the relationship with software and service providers, including contract review, performance management, and software update strategies.
• Direct the establishment of plans and tracks/reports progress against those plans.
• Direct the maintenance of the applications environment including its features, stability, availability and the processes, ensuring that each are in line with stated objectives.
• Develop and maintain an understanding of internal control, audit and systems requirements, while ensuring team, systems and procedures compliance.
• Establish and enforce software development discipline that ensures quality software that is delivered to industry standards.
• Work closely with other ITS management to assure a coordinated effort on all initiatives is presented to the university.
• Supervises and develops assigned personnel
  ➢ Responsible for hiring and training new staff.
  ➢ Provides staff with clear directions and priorities that emphasizes quality standards, service, morale building, and teamwork.
  ➢ Sets specific goals for staff that align with the strategic business objectives.
  ➢ Monitors and reviews performance of assigned personnel on a continuous (weekly, monthly, quarterly and yearly) basis.
  ➢ Develops and coaches assigned personnel to systematically assure the highest quality service.
  ➢ Advises staff members in resolving problems and issues that arise with internal and external customers.
• Keeps apprised of developments in field of expertise to ensure currency and makes recommendations to senior management to improve quality, efficiency, productively and/or customer services.
• Define and develop core Business Intelligence products and services and develop roadmap, infrastructure, tools, processes and resources to support those services.
• Ensure all clients reporting and analysis deliverables are met. This includes quality reporting that is delivered in the appropriate timeframes and budgets to clients.
• Measure and monitor client satisfaction (internal and external) to ensure we are meeting and/or exceeding client expectations.
• Develop and improve processes and metrics, coordinate with data management team to automate, drive efficiencies and adhere to proper data security guidelines and policies.
• Knowledge of and experience in developing and documenting security architecture and plans, including strategic, tactical and project plans
• Must be able to manage complex information security projects; understand and assess document control and repositories in databases; assimilate the concept of new applications and relate them to the overall organization computing/communications environments; and coordinate and develop solutions to complex problems in a multi-user environment.

Qualifications/Skills:
• Bachelor's degree in Computer Science/Information Systems, Business Administration, required.
• Eight (8) years experience in information technology, required.
• Three (3) years experience in data warehouse and business intelligence systems required.
• Four (4) years experience in IT security and security management required.
• Five (5) years management experience, with knowledge of business and management principles involved in strategic planning, resource allocation, leadership technique, and coordination of people and resources, required.
• One (1) year of experience working in a University environment, preferred.
• Experience and knowledge of ERP systems, the PeopleSoft Suite, hosting solutions and how to use technology and applications to solve business problems.
• Demonstrated skill with Oracle PL/SQL, stored procedures, SQL optimization.
• Technically fluent in programming languages, including PeopleCode and PeopleTools
• Working knowledge of database design and file management techniques.
• Demonstrated knowledge of the Software Product Development Life Cycle Methodologies.
• Detail oriented with demonstrated project management experience and/or substantial exposure to project-based work structures, project lifecycle models, etc.
• Excellent written and verbal communication skills.
• Demonstrated problem solving skills using logic and reasoning to identify the strengths and weaknesses of alternative solutions, conclusions or approaches to problems.
• Demonstrated skill in systems integration examining and reengineering processes, formulating policy, and developing and implementing new strategies.
• Skill in budget preparation and fiscal management.
• Ability to perform various tasks simultaneously and work in a fast-paced environment, while producing optimal outcomes.
• Flexibility and the ability to operate under stressful, time-sensitive deadlines.
• Excellent customer service orientation required and ability to facilitate resolution to questions and concerns with internal and external customers.