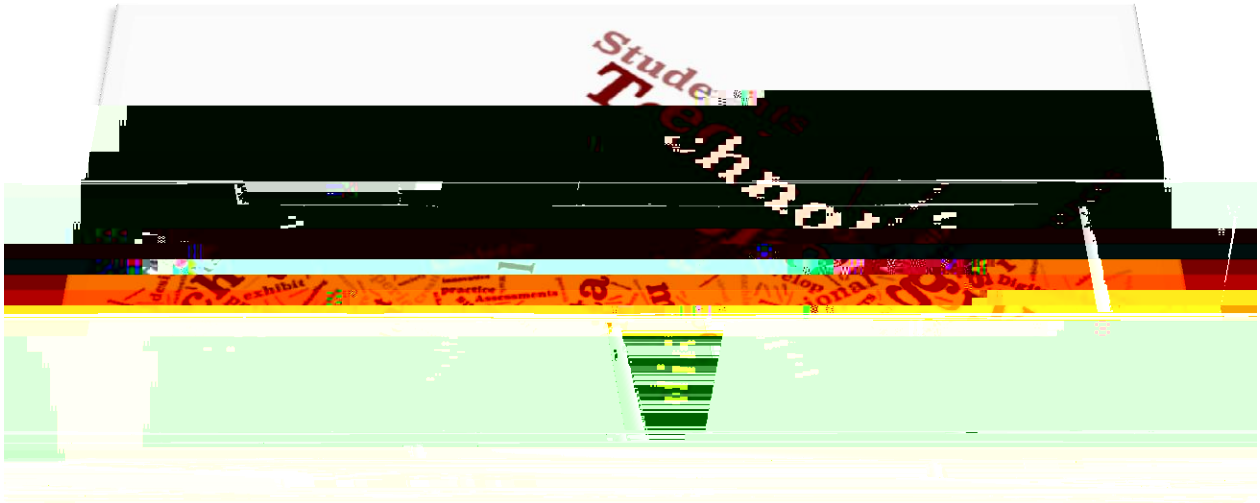
Imperial Community College District

Strategic Technology Plan 2011-2015



Committee DRAFT: Version March 28, 2011

We shall provide technology-rich learning and working environments that promote the acquisition and use of 21st Century Skills.

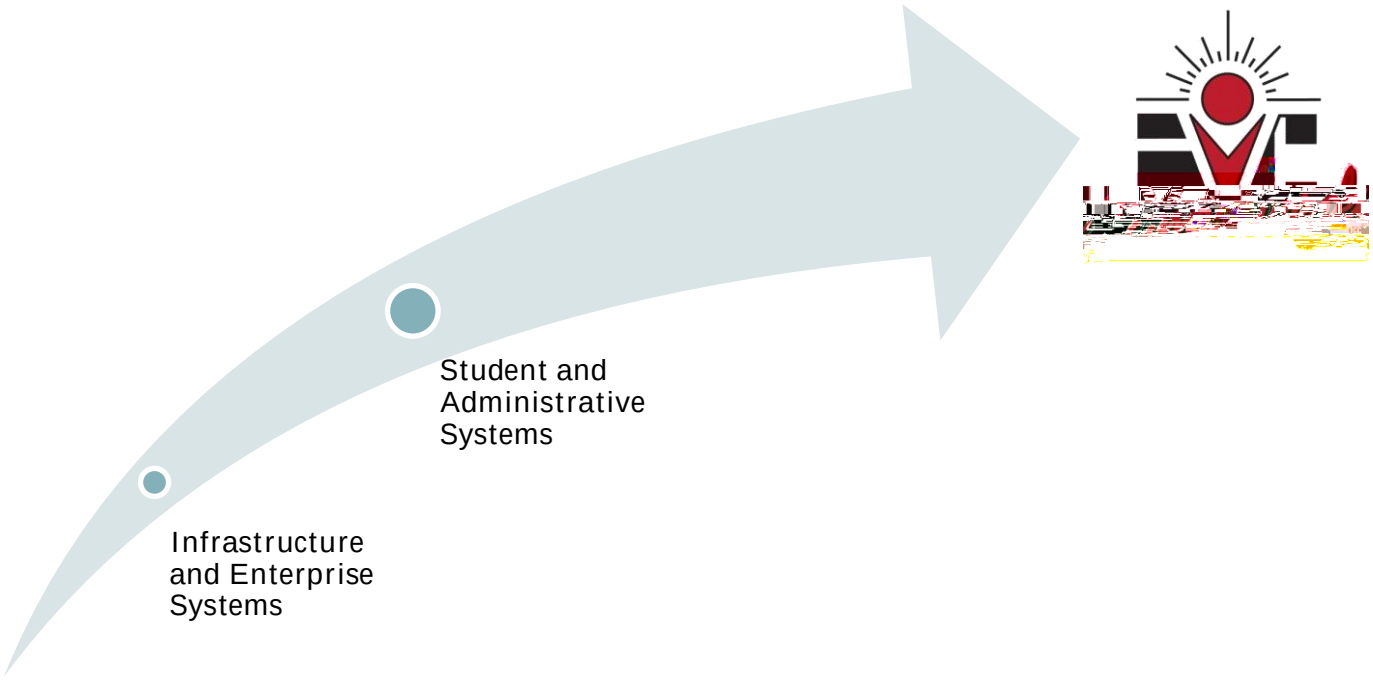
Principles in Support of Initiative Two
1. Appropriate technologies, tools, and content is readily available
2. Technology renewal and replacement is on predictable cycles
3. Faculty/staff-driven principles for selecting and deploying technologies
4. Actively embrace student technology use

We shall implement and support enterprise data systems that support effective decision-making and promote synergy, collaboration, and efficiencies throughout the organization.

Principles in Support of Initiative Three
1. Highly utilized enterprise-wide learning management systems
2. Best of breed student information and administrative systems
3. Leveraged cloud computing and data warehouse models
4. Secure authentication, authorization, and provisioning

We shall provide support structures that encourage confidence and success for all users.

Principles in Support of Initiative Four
1. Just-in-time support
2. Best of breed web support and documentation
3. Diverse learning options
4. Actively promote use of communities



In October 2010, IVC was awarded a 5-year federal Title V grant focused on innovative approaches to teaching through technology. The *Access to Technology Leads to Advancement and Success* (ATLAS) program provides support resources toward the implementation of this strategic plan. This plan will incorporate the goals and objectives of the ATLAS grant each year.

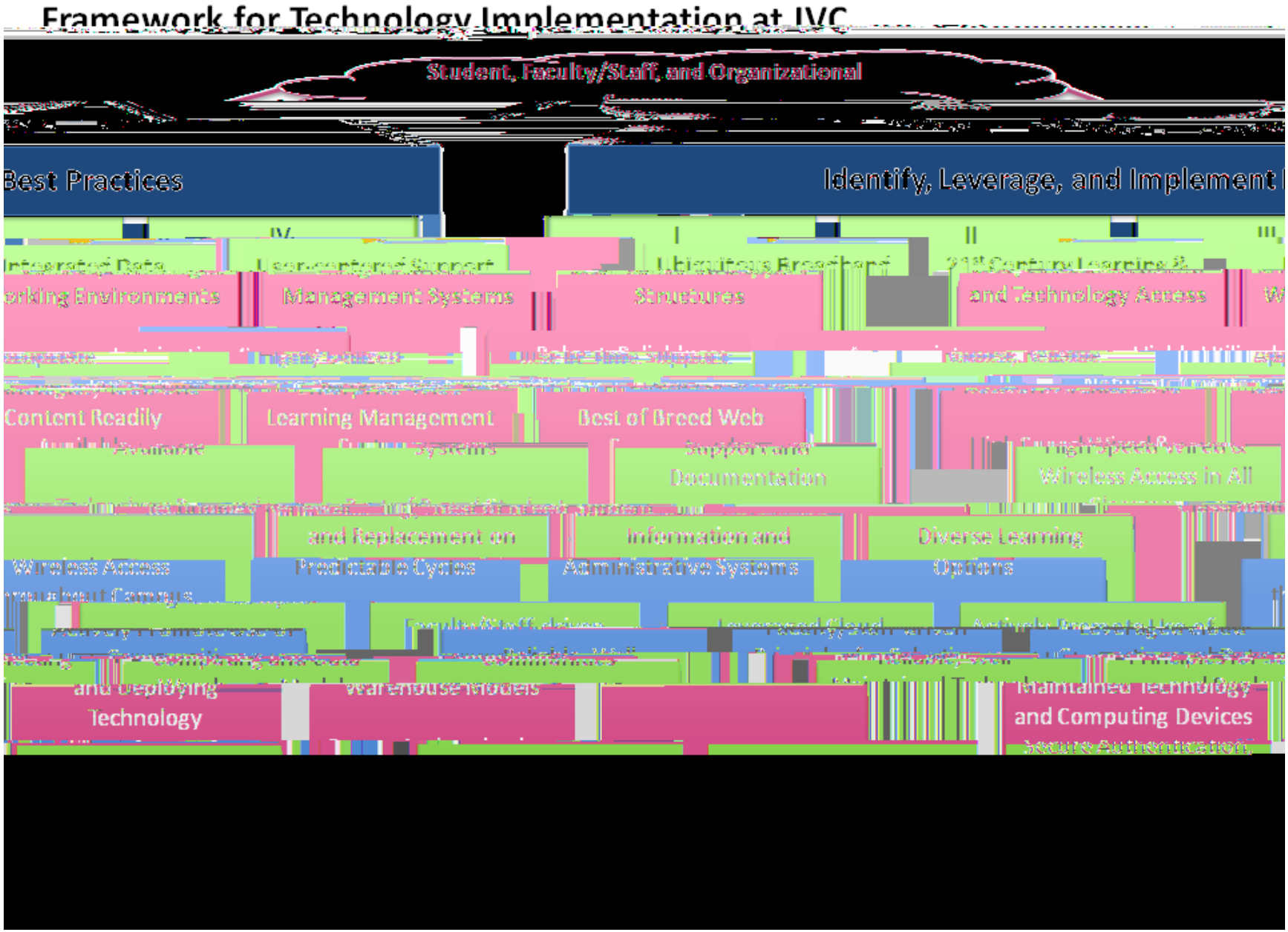
In addition to the ATLAS grant, IVC is currently undertaking major modernization and facility improvements, which is supported by the passage of Measure J in November 2010. The modernization and construction of new facilities will span the next 7-10 years. It is imperative that this Strategic Technology Plan coordinate with these activities to maximize funding and provide for an integrated implementation of technology on campus.

2011 Action Plan

The following activities are outlined for calendar year 2011.

IMPLEMENTATION			EVALUATION	
Activity	Lead Person(s)	Support Index Map	Evidence	Completion Process
1. Clarify purpose, standards, membership, and meeting schedule of Technology Planning Com	Todd	4.1	Meeting minutes, membership roster and meeting schedu	Submitted to Executive Council - January 2011
2. Evaluate the current status of the campus infrastructure, enterprise systems, and support structures	Todd	1-4	Report	[redacted] Council - May 2011
3. Develop Strategic 5-Year Technology Plan (to include comprehensive budgeting, maintenance, refresh of technology)	Todd	1-4	Report	Submitted to Executive Council - June 2011
4. Develop comprehensive plan for campus-wide wireless network	Jeff E.	1.2	Documentation (as built)	Submitted to Executive Council - June 2011
5. Fully implement systems management appli (KACE) and develop policies and procedures for its us	Gordon	1.5, 1.6, 1.7	Documentation (as built)	Submitted to Executive Council - April 2011
6. Improve reliability and security of IVTA and C Connections	Jeff E.	1.2	Documentation (as built)	Submitted to Executive Council - March 2011
7. Implement industry-standard network security an monitoring practices	Jeff E.	1.1, 1.9, 1.10	Documentation (as built)	Submitted to Executive Council - June 2011

20.Improve integration of instructional systems (Gradebook, LMS, Faculty Website) with suppo for Faculty and Student Use	Jeff E./Omar	3.5, 3.9, 4.3, 4.4	Documentation (as built)	Submitted to Executive Council - June 2011
21.Conduct Security and Service Audit	Todd	3.3	Report	Submitted to Executive Council - December 201(
22.Conduct redesign of website Improvements public (external) and private (internal) web pres	Omar			


Framework for Technology Implementation at IVC
Student, Faculty/Staff, and Organizational
Best Practices
Identify, Leverage, and Implement
IV
I
II
III
Management Systems
Structures
and Technology Access
Content Readily
Learning Management
Best of Breed Web
Documentation
Wireless Access in All
and Replacement on
Predictable Cycles
Information and
Administrative Systems
Diverse Learning
Options
Wireless Access
and Deploying
Technology
Warehouse Models
and Computing Devices

Appendix B

2

	Deficient Support Capacity a	Limited Support Capacity and Efficiency	Satisfactory Support Capacity an	Exemplary Support Capacity and Efficiency
1.1				

	Deficient Support Capacity a Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity an Efficiency	Exemplary Support Capacity and Efficiency
1.6 Imaging Software	, P D J L Q J 6 R I W Z D U	Imaging software is used in the primitive sense only providing recovery services with the imag software provided by the vendor.	An image is used for delivery of t P D F K L Q H E X W L V Q ¶ the software on the machine. Onl basic OS and basic software is imaged. Imaging is used as a troubleshooting strategy.	Imaging software is used f delivery of new machines, and as troubleshooting strategy. Softwa installed through the imagi process is comprehensiv
1.7 Metering and Application Push Technology	Metering and Push technolog L V Q ¶ W X V H G D V	Metering and Push technology use G I R U P H W H U L Q J installation and updates, and its is limited in scope.	Metering and Push technology is for metering and some software updates, but major software installations are handled on the individual computer.	Metering and Push technology is used for all software distribution, technical updates, and for meteri R I V R I W Z D U H X V H R computers.
1.8 Thin-client Computing	Thin- F O L H Q W F	Thin client is used but is limited small number of uses for specific applications.	Thin client is used for most users administrative systems and some productivity software.	All administrative and productivity software for staff is delivered through a thin-

2

2

Deficient Support Capacity ar Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	

2

	Deficient Support Capacity a Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
4.5 Trouble Ticketing System	No trouble ticketing system exists.	A simple trouble ticketing syste in S O D F H E X W L V Q is simple in its implementation, allowing for universal tracking o issues and establishing trends.	A trouble ticketing system is in plac is used extensively for responding technical issues. Analysis of issues response times, and possible trend L V Q R W effectively.	All technical issues are recorded and delegated to appropriate resources through an electronic trouble ticketing system. All technical issues are tracked and evaluated through this system.
4.6 Use of Online Knowledgebase for Technical Help	Staffs seek no help from onlin help both due to availability o resources and district culture	Some staff seeks online help, b W K H E H K D Y L R U L V resources are limited.	Many staff seeks online help and there are several broad resources available. Use is not organizationa pervasive.	Most staff seeks help from online knowledge bases as their first resource for help from diverse ar comprehensive resources. This i pervasive part of the culture.
4.7 Software Support Protocols and Standards	No list of supported software provided for users.	A list of supported software is provided, but no differentiation made for the kind of support a category of software will receiv	A list of supported software is provi and differentiation is made for the l support a given category of softwa U H F H L Y H K R Z H Y H U different processes closely.	A list of supported software is provided, with clear differentiat support processes for each set o software that are consistently us
4.8 Documented Procedures				

2

	Deficient Support Capacity a Efficienc	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
4.10 Differentiated Job Descriptions	Technical support employees it all creating redundan and inefficiencies.	Technical support employees d D O O E X W U H G X Q C due to size and/or staffing leve	Some differentiation in jobs has R F F X U U H G D O W K R X provided based upon skill competencies.	Job descriptions are fully differentiated creating specialization and efficiencies, a a clear avenue for support.
4.11 Retention	Employee turnover is high primarily due to low employe satisfaction.	Employee turnover is high prim due to other employment opportunities.	Employee turnover is moderate (excluding retirement), and employ satisfaction is good.	Employee turnover is low (excluding retirement), and employee satisfaction is high.
4.12 Competitive Compensation	Technical positions are poorl competitive, offering compensation in the bottom 5 of equivalent organizations in area.	Technical positions are modera competitive, offering compensa in the 50th to 75th percentile of equivalent organizations in the area.	Technical positions are competitive,	

2

Deficient Support Capacity ar Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	

Executive Summary

Imperial Valley College (IVC) was evaluated on their overall Technology infrastructure to analyze possible flaws in the architecture and minimize the risk of a security breach. This assessment focuses primarily on data networks and enterprise systems such as servers and dedicated appliances.

Each segment of the assessment will have a severity level assigned. IVC should use these levels to prioritize the work that needs to be done after the completion of the assessment. The following levels will be used throughout the document:

- x : This priority suggests that these areas should be addressed first and represents a potential security concern.
- x : This level of priority represents findings or configuration changes that will enhance the performance of existing systems, but they don't represent a significant security concern.
- x : The areas marked with this priority are findings that should be addressed when resources are available.

C

IVC's internal network has multiple VLANs created to isolate layer 2 broadcast domains. Connections between switches are trunked to allow multiple VLAN traffic to return to the core and out to the Internet. All switches appear to have the spanning-tree protocol turned on, which helps prevent network loops in the topology. Network ports where an IP phone is connected should also be configured as a trunked port to allow a computer to connect to the phone. The following are some low-level priority recommendations:

- x

x E-

End-user accounts and passwords are created and assigned by the technology department. This practice is very common for IT shops, although it does not scale well and has a potential for a security breach. Some end-users are aware that they have the capabilities to change their own password, while many others call the IT staff to have their password changed. IVC may want to follow these recommendations:

- Create policies and procedures around the use and maintenance of passwords. They should outline clear expectations around the use of passwords, change mechanisms, length and strength, resetting, age, etc.
  Severity level = Moderate
- End-user should be given a generic (but secure) password when the account is created and force them to change the password the first time they log in.
  Severity Level = Suggested
- Tech staff should use their own account to access staff computers for troubleshooting and maintenance.
  Severity level = Moderate
- Provide users with clear instructions on how to change passwords. The IT staff should promote good security practices to end-users and encourage them to change their passwords frequently.
  Severity level = Suggested
- IVC may adopt a policy to have passwords change every certain period. For example, users are forced to change passwords once a year.
  Severity level = Suggested
- Enforce password policies via Active Directory Group Policies.
  Severity level = Suggested
- IVC should determine the appropriate level of staff authorized to change user passwords.
  Severity level = Moderate

Severity Level = Critical

Most if not all the Windows servers in the IVC campus are accessible via the Microsoft's Remote Desktop protocol (RDP). This easy-to-use tool allows IT staff to access the server console to perform administrative tasks. Because the servers are located on the same internal network as faculty and staff, extra security measures need to be taken so that servers are not exposed to unauthorized access. In reviewing the Active Directory Users and Groups, it does appear that IVC has created a special security group that is used to control RDP access to the servers. IT staff need to ensure each server is configured so that only authorized access to servers occurs via RDP. This same philosophy should apply to the local server security roles; only the authorized groups should have administrative privileges over the server to minimize the potential of a security breach.

IVC uses the Sophos anti-virus solution to protect desktop and server computers. A handful of old servers continue to run the Symantec product, which appears to be the prior version of anti-virus software being used. During the discovery process, for the most part all servers and workstations had the Sophos agent installed and signature files up-to-date.

- IT staff should provide administrations with periodic reports from the anti-virus management platform. Examples of such reports are: (Severity Level = Suggested)
  - Compliance reports (protected systems, signature files)
  - Threats that have been mitigated
  - Top tens
  - Attack vectors (Trojans, e-mail, phishing, key loggers, etc.)
- Signature files should be updated regularly throughout the day and should balance between resources available and the acceptable risk. The larger the number of systems, the more network traffic and resources are needed to keep all systems with current signature files.
  Severity level = Moderate
- IVC should also build capacity to deploy an anti-virus solution that covers other operating systems other than Windows. A good example is the web server that runs a Linux operating system.
  Severity level = Suggested

IVC owns the KACE KBOX appliance that allows for the management of desktop lifecycle. This multi-function appliance provides technical staff with tools to effectively manage desktops and perform several tasks such as:

- Perform and maintain computer inventory (hardware and software)
- Software distribution
- Remote support tools
- Schedule and deploy security patches, system updates or new releases
- Ticket management
- Power management

During interviews with staff, it does not appear that IVC has embraced the tool to its full potential. Desktop and server patching is an ad-hoc approach and not very effective. The following could assist in the process:

- Assess the current functions the KBOX is currently doing and develop a plan to allow the appliance to bring additional efficiencies.
  Severity level = Moderate
- Develop a deployment strategy to include key staff and a realistic time frame for full implementation. The plan should progressively implement features of the KBOX appliance until they satisfy the needs of IVC.
  Severity Level = Moderate
- Provide adequate training for technical staff on the use of the appliance. Severity Level = Moderate

Back-end Services

IVC runs Microsoft Active Directory (AD) to run directory services for the campus. Two Windows 2008 servers are running AD in a clustered environment and replication seems to be working well. Internal DNS is currently integrated into the AD infrastructure although some issues were found with internal DNS replication. Both AD servers are running as Global Catalog servers (GC), which is a desired environment to

provide resiliency. The following key recommendations need to be followed to correct existing issues and avoid potential problems in the future:

- Raise the AD Forest/Domain functional level to Windows 2008. It's currently running at Windows 2003 functional level.
  Severity Level = Moderate
- Have the operations master server (IVC1) synchronize its clock with a reliable NTP server. Since all client computers synchronize their time to this server, it is critical that this server's clock is as accurate as possible. Currently it shows a difference of approximately 2 minutes. The following link provides instructions on how to do this: (Severity Level = Critical)
  http://support.microsoft.com/kb/816042

Severity Level = Critical

Recommendations redacted due to security concerns.

- Accessing servers via the console or remotely.
- Adding computers to the domain.
- Manage user accounts and groups.
- Server patching or updating.
- Manage network services such as DHCP and DNS.

Recommendations redacted due to security concerns.

Similar to the DA account, Active Directory contains Domain Administrators Group (DAG). This group shares the same administrative privileges to the DA account. Only high-level managers that require unrestricted access to manage the directory should be part of this group. The college should strongly consider the following suggestions:

- Change the DA account password as soon as possible. This account credentials should only be held by key personnel at IVC. This password should be changed on a regular basis (every year at minimum).
- *Recommendations redacted due to security concerns.*
- Review the members of the DAG group and remove anyone that doesn't have a need to manage the directory services. Special consideration should be given to consultants and ex-employees.
- It appears the college has created an IVC Admins group and is encouraged to implement and use such group to manage servers and day-to-day operations of the enterprise infrastructure. This group could have local administrative privileges on servers, allowing members full administration using their domain account.
- Implement delegation at the Organization Unit in AD. This allows a technician or employee to have certain administrative access over certain portions of Active Directory structure. This minimizes exposure to the enterprise infrastructure and provides the flexibility of having multiple staff managing the directory services in their respective political domain.

Severity Level = Moderate

IVC uses a Windows 2003 server to provide dynamic IP addresses to client computers. IVC should consider the following recommendations:

IVC currently runs a centralized print server where all printers are connected. Users then connect to this server and choose the appropriate printer on the network to use. The servers currently running this operation are 6 to 7 years old. IVC should consider replacing or virtualize the server to avoid potential downtime for all users.

Severity level = Critical

IVC currently uses Backup Exec as their platform to perform data backups jobs. The IVCBK1 server is running Windows 2003 with the Symantec Backup Exec version 12.5. This enterprise platform does appear to have a Microsoft Exchange plug-in that allows the system to backup the message store while online. Another server named VM2 is used as a file server to store backups for the Banner system.

- Backup files are being stored in external storage attached to the backup server.
- There are four different backup jobs:
    - Data and Infrastructure – Daily
        - *f*

- IVC should implement an off-site backup strategy to transport critical information outside the campus environment if possible.
  Severity level = Moderate
- The backup server appeared to have external USB drives connected for additional storage capacity. USB interfaces may not be adequate for fast data transfers or as reliable as SCSI or SAS interfaces. IVC may want to consider upgrading these storage devices.
  Severity level = Suggested

E-mail System

IVC currently hosts Microsoft Exchange server as their electronic messaging and collaboration platform. Exchange 2007 currently serves approximately 500 mailboxes for staff and faculty that are primarily accessed via the Microsoft Outlook client.

End-users may also access the Exchange system via the Outlook Web Access (OWA) web interface, which allows users to check e-mail with a standard web browser. This also provides the framework for users to access their e-mail through mobile devices via Active Sync.

IVC uses the Barracuda Spam Firewall appliance to filter inbound and outbound mail for spam and viruses. End-users have the option to customize their filter settings to accommodate specific needs outside the general configuration settings of the filter.

The Microsoft Exchange 2007 server currently has all 4 roles installed within one server (Hub, Transport, Client, Mailbox). This setup is common and adequate for an organization the size of IVC. Exchange services run on a Dell PowerEdge 2950 running Windows 2003 server with 8 GB of RAM and 6 x 146 GB (15K) hard drives. The server was installed in 2007 and has 4-hour on-site premium warranty that expires in May of 2012.

Severity Level= Critical

IVC currently has no per-mailbox storage limitations configured in the system defaults settings. Space on the hard drive is currently at two-thirds capacity and IVC runs the risk of filling the hard drive space very quickly. IVC should do an assessment of space per mailbox and perform capacity planning to avoid running out of disk space.
The following command can be used in the Exchange Management Shell to provide a list of mailboxes sorted by size. Unfortunately, Exchange 2007 does not provide this feature via the GUI:

Get-MailboxStatistics | Sort-Object TotalItemSize -Descending | ft DisplayName,@{label="TotalItemSize(KB)";expression={$_.TotalItemSize.Value.ToKB()}},ItemCount

The first storage group where all the mailboxes reside is currently close to 200GB and most mailboxes are at approximately 1.5 GB of space

- Upgrade the firmware on both spam firewall appliances. The latest firmware update will consist on a major upgrade to Version 4.x which provides a new streamlined interface, new features and bug fixes.
  Severity level = Moderate
- Create a new DNS record for the outbound mail instead of oldspam.imperial.edu.
  Severity level = Moderate
- Configure the appliance for LDAP/Exchange user integration. This feature provides two important

Next Steps

This document can serve as a guide to administration on the next logical steps to enhance security and improve uptime and reliability. The perimeter network should be the first area of focus and ensure only necessary network traffic is allowed. The second area of focus should be on the need to improve the enterprise infrastructure such as servers, data backups, storage systems, Active Directory and other back-end systems. The third area of focus should be to strengthen internal security and access to critical systems such as the financial and student system.