**SOP – Client Due Diligence**

1 Firm Overview 2

2 Regulatory Compliance 2

3 Known Issues 2

4 End user Support Expectations 3

5 Data Backup and Archiving 3

6 Business continuity requirements 3

7 Disaster recovery requirements 3

8 Security Posture 4

8.1 Technical Controls 4

8.2 Monitoring and Logging 4

8.3 Documentation and Auditing 4

8.4 End user Training and process controls 4

9 Software Applications 5

10 Infrastructure overview 5

10.1 Hardware 5

10.2 Telecom, WAN and Remote Access 6

10.3 Active Directory and Account management 7

# Firm Overview

Please provide

* Business description
* List of locations
	+ Do any locations require scheduled on-site visits?
	+ Are there restrictions we should know of in terms of access, insurance requirements, dress code etc?
	+ What are your hours of operation?
	+ Number of employees at each location
* Number of
	+ Desktops
	+ Laptops
	+ Server instances
	+ Locations
	+ Amount of data in one full backup, how long do we need to keep backups?
* Users
	+ Full computer users (desktop or laptop)
	+ Mobile users (phones, tablets with more than just e-mail)
	+ E-mail only users
* On site requirements
	+ As needed ok or is full time presence required?
* Number of new hires last year, projected new hires for the coming year.

# Regulatory Compliance

What regulations are you subject to which impact your information technology management needs? E.G.

* Health Insurance Portability and Accountability Act
* ARRA meaningful use
* The Sarbanes Oxley Act
* Federal Information Security Management Act of 2002 (FISMA)
* Family Educational Rights and Privacy Act (FERPA)
* Payment Card Industry Data Security Standard (PCI-DSS)
* Gramm Leach Bliley Act (GLBA)
* California Privacy Act
* SEC 17 [CFR 248.30](https://www.ecfr.gov/cgi-bin/text-idx?SID=226b4b62d8bf25d29cc88df5039cddde&mc=true&node=se17.4.248_130&rgn=div8) (data protection policies), [17 CFR 240.201-202](http://www.ecfr.gov/cgi-bin/text-idx?SID=5621786ec1a831400e4b64f3e92198bd&mc=true&node=pt17.4.248&rgn=div5#sp17.4.248.c) (protections against identity theft), and [17 CFR 240.17a-4(f)](http://www.ecfr.gov/cgi-bin/text-idx?SID=b6b7a79d18d000a733725e88d333ddb5&mc=true&node=pt17.4.240&rgn=div5#se17.4.240_117a_64) (preservation of records)

# Known Issues or “Pain Points”

What information technology issues are currently impacting business operations? For example

* Inadequate end user support
* Roaming profiles in place but not working
* Slow or unreliable in-office system performance
* Remote access systems which are slow or cumbersome?
* Inadequate strategic guidance e.g. around infrastructure, security, regulatory compliance?
* Missing system functionality e.g. filesharing, encryption, collaboration tools?
* Business interruptions due to system downtime incidents?
* Inadequate disaster preparedness?
* Inability to meet regulatory security requirements or obtain needed certifications / attestations for clients or investors

# End user Support Expectations

* How many end users will need to be supported?
	+ Full time office employees
	+ Scouts that have lower end user support needs
* What are your end user training needs?
* What are the typical support requests which come in?
* Is there an export from an internal ticketing system we can use?
* What are the on site expectations staff has?

# Data Backup and Archiving

* What is your current backup arrangement?
* Is information stored on workstations and laptops that can not be lost – or is this all a copy of information stored on your servers?
* Once a file or e-mail message has been deleted by a user, how much of a grace period do you need before that file is gone beyond the ability of an administrator to recover it from a backup?
	+ 30 days
	+ 90 days
	+ 1 year
	+ 7 years
* Do you require archiving of e-mail, user instant messaging logs or social media posts?

# Business continuity requirements

Please describe your business continuity / system availability requirements?

Are there systems with exceptional uptime requirements that we should know about? E.G.

* life support systems
* environmental control systems
* security systems
* e-commerce systems

# Disaster recovery requirements

Please describe your disaster recovery requirements.

Do you have regulatory or contractual obligations which govern your disaster preparedness needs?

# Security Posture

Please indicate which of the following security measures are in place in your environment. Are there measures which are not in place which need to be?

## Technical Controls

* Workstations requiring complete lockdown to prevent user changes
* Password management policies
* User Identity management / federation systems
* Server and Workstation Patching
* Network device firmware patching
* Endpoint encryption
* Internet Traffic Filtering
	+ Do you require limited access for a subset of users?
* Data loss prevention – i.e. traffic filtering to control the flow of sensitive information such as social security or credit card numbers
* Two factor authentication
* Mobile Device Management
* Switch port access controls
* Role based access controls to sensitive data

## Monitoring and Logging

* Server and network device log aggregation
* Employee activity logging systems
* Intrusion detection systems

## Documentation and Auditing

* Written security management plan
* Written disaster preparedness / business continuity plan
* Written incident response plan
* Acceptable use policies
* Recurring self-assessments
* Recurring Third party security audits
* Sensitive data storage audits
* Pentration testing

## End user Training and process controls

* User security awareness training
* Proactive e-mail phishing or other white hat social engineering testing
* Funds transfer fraud controls

Please describe any particularly sensitive data access requirements we should be aware of?

Is any of your infrastructure shared with another company for example a subtentant? E.g Oakland Raiders

# Software Applications

* Please list all line of business applications in use including SaaS applications.
* Is any of your software custom developed for your business?
* Is all software currently supported by the developing firm?
* Does all software which has to be available 24 x 7 for your business, have 24 x 7 support from the developer?
* Is any software dependent on
	+ Connecting to a server based on a fixed name or IP address that can not change?
	+ Use of a physical security dongle
	+ Running under a particular account in the console session of a server
* Applications which run inside a DOS shell?
* Software which performs synchronization (e.g. file synchronization from desktops to servers or from server to server across a WAN link, software which synchronizes personal calendars, contacts or mail to a public store or vice versa)
* Software which must be manually started after the computer running it is rebooted. We are particularly concerned about software which provides support for several systems, e.g. a Point of Sale management package supporting several POS terminals.
* Do any applications maintain their own user accounts, apart from Active Directory?
* Are you using any third party plug-ins to G-Suite products?
* Are there business critical applications whose failure might not be immediately noticed and which must therefore be tested manually after any change to the network to ensure they are working?
* Is the availability of any application protected by means other than server clustering at the hypervisor layer – e.g. transaction log shipping, SQL clustering, Windows operating system clustering etc?
* Is there software with known issues requiring special care e.g. servers which must not be restarted, which must be restarted in a certain order, software which requires manual intervention following any server restart?
* Is there software running under an account whose name or password must NOT be changed?

# Infrastructure overview

## Hardware

* Servers
	+ Hostname
	+ Location
	+ Operating System
	+ Key software
	+ RAM
	+ CPU
	+ Total Disk space
	+ Used disk space
	+ Role (mail server, accounting server, line of business application etc)
	+ If virtual, Hypervisor host server name
	+ If physical, model, year of purchase
* Storage
	+ Name
	+ Location
	+ Total Capacity
	+ Used capacity
	+ Manufacturer, model, purchase date
	+ Role – data backup storage, hypervisor back end storage etc
* Workstations
	+ Hostname
	+ Type (laptop, desktop, tablet)
	+ Primary location
	+ Operating System
	+ MS Office version (if applicable)
* Network Equipment
	+ Name
	+ Type (firewall, routers, access point, switch)
	+ Location
	+ Manufacturer
	+ Model
	+ Year of purchase

## Telecom, WAN and Remote Access

* WAN connections
	+ Location
	+ Vendor
	+ Bandwidth
	+ Technology (Cable, T1, Microwave, Ethernet over Copper, Fiber)
	+ Service Type(s) (Internet, Voice, Dedicated)
* What type of remote access systems do you have in place?
	+ Web based access to e-mail or line of business applications?
	+ VPN
	+ Citrix or Windows remote Desktop
* Phone system
	+ Manufacturer name
	+ Where is the main PBX located? Is this a hosted system?
	+ Is there an active support agreement for this system?
	+ Is traffic passing over connections for which QoS controls are not in place?
	+ Are there integrations between the phone system and other systems?

## Active Directory and Account management

* How many Active Directory domain are present in your environment?
* Are there any non-windows directory management systems in place?
* Are end user passwords known only to themselves?
* Are shared accounts in use?
* Do you have a requirement for users to change passwords periodically?
* Are there computers in your network which are not part of your domain?

**10.4 Application Monitoring**

* What is the name/nature of the application?
* Is the application a COTS application or was it developed internally?
* Does the application have an API or CLI?
* Does the application support SNMP or other standard protocols?
* How do you monitor the application today?
* What separate components are involved in the delivery of the application (URLs, services/processes, sub-applications, databases, etc.). How do the pieces fit together?
* Can the application be monitored directly, via one of the methods, or must it be monitored anecdotally? For example, we may not be able to directly poll for performance but may instead parse the application's log files for error messages.
* Describe a recent event which had a real business impact, and which you discovered the hard way. Did the post-mortem indicate a way to avoid a repeat in the future (e.g. If only we were monitoring the X)?
* Does the application run stand-alone or in a cluster? Is there a single point of failure? What percentage of impairment can you tolerate before you want a phone call at 2AM?