

July | '11

*Testimony for the*  
Department of Labor  
2011 ERISA Advisory Council

Privacy and Security Policy

**GuidedChoice.com, Inc.**  
**Thomas J. Condrón**  
Executive Vice President  
Client Relationships

---



## Table of Contents

<b>GuidedChoice .....</b>	<b>3</b>
<b>Knowledge and Preparation .....</b>	<b>3</b>
<b>Implementing Flawless Policy Builds Upon Ingrained Ethics .....</b>	<b>7</b>
<b>Chain of Command .....</b>	<b>7</b>
<b>Our Mission and Our Responsibility .....</b>	<b>9</b>
<b>The 1<sup>st</sup> Line of Defense is Policy .....</b>	<b>10</b>
<b>Security Audit Policy .....</b>	<b>11</b>
<b>Risk Assessment .....</b>	<b>12</b>
<b>An Evolving Protection Plan .....</b>	<b>13</b>
<b>Appendix .....</b>	<b>15</b>



Chairman Rappaport, Vice Chair Barnes, and the 2011 ERISA Advisory Council Members, thank you for the opportunity to present the security policy implemented successfully at GuidedChoice. My name is Tom Condrón; I am the Executive Vice President of Client Relationships at GuidedChoice.

### **GuidedChoice**

At GuidedChoice we have established a business built upon a culture of openness, trust, and integrity. Through these practices we have maintained a company committed to protecting our employees, partners, clients, and the company from all illegal or damaging actions taken by individuals knowingly or unknowingly. Our company is one of the leading investment advice firms, providing reliable service to over 78,000 defined contribution plans with more than 4 million participants. As GuidedChoice continues to grow, and our client numbers expand, we continue to implement the top of the line security measures to ensure our clients' information remains secure. In this technology booming era, network security must perform flawlessly without pause. At GuidedChoice we pride ourselves on our Privacy and Security Policy. We have employed a certified Security Manager on staff and constantly have our clients' confidentiality in mind.

### **Knowledge and Preparation**

The growing rate of technology has been exponential since the first computers. In the past, computers weighed close to fifty pounds and information was slowly typed in fluorescent green text on a black buzzing screen. Now we carry virtually weightless mobile devices that have hundreds of times the operating power compared to the first generation computers. We don't think twice about emailing, banking, buying music, or downloading new software on our phone while casually riding to work. The next generation communicates and operates while on the go. The issue with this booming technology is keeping our secure information from being corrupted or breached. According to Frost & Sullivan of the (ISC)<sup>2</sup> Global Information Security Workforce, "The three primary new technology trends studied

in detail in 2010 were mobile devices, cloud computing, and social media. These new technology areas also represent the greatest risk to organizations.”<sup>1</sup> While the growing technology makes communication more convenient and boosts available productivity, the ability to maintain secure information is becoming exceedingly difficult.

There is an on going debate regarding the security measures taken to protect against the growing data vulnerability risks. We expect this area to be one of constant change and improvement. The Internet Policy Task Force, under the Obama administration, has come up with a proposal to help organize stronger security standards for our online personal identifiable information (PII). In an article written by previous Chief Counselor during Clinton’s Administration, Peter Swire states that, “Secretary Gary Locke’s green paper ‘Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,’ is pushing to create a Privacy Policy Office.”<sup>2</sup> The Internet Policy Task Force proposes to provide an office to house a department to regulate better security measures,

“The proposed PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together; and it would work in concert with the Executive Office of the President as the Administration’s lead on international outreach for commercial data privacy policy. The PPO would be a peer of other Administration offices and components that have data privacy responsibilities; but, because the PPO would focus solely on commercial data privacy, its functions would not overlap with existing Administration offices. Nor would the PPO have any enforcement authority.”<sup>2</sup>

---

<sup>1</sup> Frost & Sullivan. “The 2011 (ISC) <sup>1</sup> Global Information Security Workforce Study.” [https://www.isc2.org/uploadedFiles/Landing\\_Pages/NO\\_form/2011GISWS.pdf](https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf)

<sup>2</sup> Peter Swire. “Getting Online Privacy Policy Right: Commerce Department Considers New Private Policy Office.” [http://www.americanprogress.org/issues/2011/01/privacy\\_office.html](http://www.americanprogress.org/issues/2011/01/privacy_office.html)



Security needs to keep up with the rapid advancements made in this technological era. At GuidedChoice we believe we have a strong defense against corruptions of any PII data we store and transfer throughout our business practices. However, given technology's rapid rate of change, it is our responsibility to continually monitor improvements to security procedures through industry relationships and organizations.

Financial advisory services need to be easily navigated by participants. This requires participants to divulge some of their personalized data, therefore there needs to be proper security measures taken to protect the exchange of personal data at all times. There is an overwhelming amount of information a participant must comprehend in order to make educated personal retirement planning decisions. Clients need the planning process to be simplified and personalized to enhance their retirement saving portfolio. In order to give our clients an easy look at their retirement plan we need to access data from multiple sources such as: a defined contribution record-keeper, a pension actuary, a stock option plan administrator, and other non-employer related sources. Although GuidedChoice has found an innovative way to provide financial advice without ever accessing a participant's personal account, we have found that having the data present is key to a participant's success in receiving and understanding our advice. Therefore we collect any necessary PII from our clients to provide them with the best financial advice possible. Concurrently, we make protecting their private data another primary objective.

Employees involved in a fiduciary program do not have a clear perception of the Department of Labor's (DOL) role in their retirement planning security; instead employees hold their employer and plan providers entirely responsible. In general our clients are overwhelmed by the plethora of financial decisions they need to make regarding their employee benefits. They have an expectation that all of their pertinent employer data be included in any retirement advice provided, including but not limited to: defined contribution, defined benefit, retiree medical, social security, any stock options, and non-qualified plans. It is true that our clients can manually add their personal data into our system, but this extra step becomes



another hurdle they do not feel comfortable jumping over. Regarding plan providers, employees expect that if their current plan is with a particular record-keeper, and their prior employer plan is with the same provider, that all of the data from both plans is automatically aggregated into the system. This can be an insurmountable challenge if the financial advisor uses a unique identifier for each separate plan. The participants must “self-identify” and aggregate the plans manually, requiring a burdensome extra step. All financial advice we provide needs to be easily accessed and processed by our clients as they near their prospective retirement age. At GuidedChoice we continue to modify our strategies of obtaining any of our client’s PII to make the process of saving for retirement convenient and productive.

Our financial advice is trusted, because as a company we provide secure and private services for all of our participants. Our clients deserve a high level of privacy for their personal information. While they do not object to their employer supplying us with their retirement plan account information, they do strongly forbid any non-plan information be provided to their employer. Therefore, our policy prevents any employee-specific data be provided to their employer that was not in the original account information given to us. By maintaining clear policies and implementing top of the line data security, we have continued to optimize our participant’s privacy.

For the typical client GuidedChoice provides an easy way to track, change, and maintain their optimal retirement plan. For those participants who are unbanked, those with little to no technology navigating skills, those with low literacy skills, those who are disabled, those acting with the power of attorney, retirees, spouses, or people with diminished cognitive skills, GuidedChoice is still capable of giving the best financial advisory service desperately needed by this specialized group. In the event that a participant falls within this special circumstance we use telephone technology. We typically use personal information questions to identify the caller. This practice is modeled after the banking industries methodology. We have never had a breach of identity with our call center. With GuidedSpending, our retirement income distribution tool, we have established an identity verification process to ensure we are speaking with the appropriate party



prior to establishing an actual distribution. For any employee seeking fiduciary advice on their future retirement, plans privacy and security are invaluable.

### **Implementing Flawless Policy Builds Upon Ingrained Ethics**

At GuidedChoice we have established a clear ethical code that is upheld by all members employed by our company. Effective ethics requires a full participation by the entire team of employees, starting at the top. Our expectations are clearly stated and maintained throughout all of our business practices. With our policy in mind, the range of people that it affects emphasizes its importance to our company. Our ethical code applies to employees, contractors, consultants, temporaries, and other workers at GuidedChoice, including all personnel affiliated with third parties. The purpose of our broad application is to uphold a clear expectation between our employees and our consumers so that all parties involved are treated with fair business practices. Security measures begin with the basic practices of our team, are enforced by our policies, and supported by our security software precautions.

### **Chain of Command**

A surge of new technology has posed a new threat to security policies and procedures. Data encryption is no longer reserved for data transferred between networks and servers; stored and transferred data now needs protection on portable media and wireless laptops. Any company that is responsible for personal identifiable information (PII) needs to be well educated on their security procedures in order to keep the confidentiality of those documents safe while they are stored and until they are expunged from any device. A responsible corporation that prioritizes in favor of optimal security should keep a Manager of Security on staff. For a larger corporation hiring or promoting personnel to take on the responsibilities of a Security Manager is easily done, however this is a challenge for smaller companies.

Third Party Administrators, small businesses, employers' Human Resource Departments, and micro-advisory firms may not be aware of the importance of



being well versed in current security procedure. To assist smaller employers and Human Resource Departments, the DOL could include security as a topic for due diligence. In order to prevent further neglect to data protection we would suggest the DOL issue a “best practices” guideline for information security. By the DOL publishing a sample security policy smaller entities would not have to dedicate their limited resources to creating a personal security procedure. Another way for smaller companies to escape added expenses would be to educate their IT manager to act as a Security Manager. By giving the IT personnel both roles, companies could focus on executing a proper security plan versus spending their limited resources on writing policy. Lastly, Human Resource Departments deal with PII on a daily basis and are often responsible for making fiduciary decisions on participant plans. With the sample security policy and a growing awareness to the importance of securing confidential information, HR Departments can act as another barrier to prevent data corruption or breach. The growing security concern can be nullified if smaller entities were better informed and security conscious while providing their professional services. Our Manager of Security has specific duties and responsibilities mentioned below; smaller entities may mirror this plan to instantly improve their data protection.

The Manager of Security is required to have a full knowledge of their firm’s Privacy and Security Policies, along with the certified skills to regulate all stored, mailed, discussed, and deleted encrypted information held by GuidedChoice. The Manager of Security implements all security policies and ensures that all GuidedChoice employees follow the developed procedures. Without a chain of command, security measures become disorganized and companies run the risk of losing important PII. Documents that should be classified as confidential could be mismarked and exchanged between networks without the proper protection of security procedures. By creating specific policy procedures, and having those procedures enforced and overseen by a Manager of Security, GuidedChoice creates another layer of protection for confidential data.

As a financial services firm GuidedChoice is privy to some of our clients’ sensitive PII beyond the information stored in their employer plan. Without the



protection and regulations provided by the HIPAA Privacy Rule<sup>3</sup>, which covers personal identifiable information given to medical personnel, all classified information gathered, recorded, manipulated, and expunged must follow a defined policy involving encryption of all confidential data. The HIPAA Privacy Rule is a great security platform for a company to emulate, however it is important that the process of aggregating data is not so onerous that participants refuse to do it. At GuidedChoice we have implemented a successful security strategy abiding by a set procedure that does not exhaust our current participants. GuidedChoice has a very specific security plan and policy; a summary of it is outlined within this testimony.

### **Our Mission and Our Responsibility**

Our mission as a trusted fiduciary institution is to provide the best financial advice possible to our clients while maintaining their privacy and securing their personal information. At GuidedChoice we believe it is our responsibility to ask the right questions about our clients' personal finances to deliver simple applicable advice relative to their current saving strategy, while obscuring our knowledge of extremely sensitive information. Employing this strategy keeps very sensitive PII such as: account numbers, where accounts are held, and any passwords to those accounts, from being transmitted through any network, and thus provides the safest form of security for our clients. GuidedChoice has the ability to work directly with our clients' financial information without exposing them to PII security risks.

The most sensitive information we collect from our clients is their social security number, their date of birth, and their home address. As a company we have minimized the personal identifiable information data we collect, while optimizing the financial advice we give our clients. Instead of accessing our clients' non-employer plan accounts, we ask our clients the balance of their retirement savings, IRAs, pension plans, etc. and the percentage they intend to continue to allocate to those accounts. With the above information we can analyze the best strategy for our

---

<sup>3</sup> Information defining HIPAA Privacy Rule policy <http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html>



clients to implement in order to enter their retirement at their desired age and income level. By asking for the minimal necessary information we need to do our job, and avoiding unnecessary and invasive questions, we maintain a very secure fiduciary model. Though the amount of PII we ask from our clients is minimal, we still apply top security measures to keep these items safe. All classified data is encrypted while in transit and while at rest (stored in the database). At the end of the day all final financial decisions belong to our clients, and we intend to empower them with the knowledge they need to implement our suggested financial advice. We don't need access to their account numbers to provide them with the very best advice possible. So, a key component of an effective Security Policy is to collect only the required information.

### **The 1<sup>st</sup> Line of Defense is Policy**

The Information Sensitivity Policy guides our staff to easily determine what information needs to be held privately within the company, and what information can be shared as public knowledge. GuidedChoice defines information as: electronic materials, company paper documents, and any information shared orally or visually (such as telephone and video conferencing). Through this policy GuidedChoice not only classifies information, but also defines how that information is to be handled, stored, mailed, or expunged while it travels through our records.

The process begins with identifying information as either *GuidedChoice Public* or as *GuidedChoice Confidential*. For any material to be deemed *GuidedChoice Public* it must have been declared as such by someone with the authority to do so. All materials deemed *GuidedChoice Public* have been assessed and cleared of causing any damage to our clients and our corporation, so those documents may be freely shared with anyone. *GuidedChoice Confidential* requires more sensitive and detailed methods of operation.

*GuidedChoice Confidential* is information that should be protected very closely such as: trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company, as well as personal



identifiable information (PII). Also included in *GuidedChoice Confidential* is information that is less critical, such as telephone directories, general corporate information, personnel information, and other materials that do not require as stringent a degree of protection. Within the overarching category of *GuidedChoice Confidential* there is a subcategory defined as *GuidedChoice Third Party Confidential*. This is confidential information belonging or pertaining to another corporation, which has been entrusted to GuidedChoice by that company under non-disclosure agreements and other contracts. All documents under the umbrella classification of *GuidedChoice Confidential* require GuidedChoice personnel to follow company policy and all commercially reasonable methods to properly secure the information. All security questions may be directed to our Manager of Security.

### **Security Audit Policy**

GuidedChoice has many layers built into securing documents pertaining to our business. Our policies are built to protect confidential information belonging to the company, our customers, employees, contractors, consultants, temporaries, and third party personnel. Therefore, at GuidedChoice we have established further security procedures beyond the above-mentioned practices. Our Manager of Security has the authority to conduct a security audit on any system at GuidedChoice, along with any device that is present on GuidedChoice premises, but may not be owned by GuidedChoice. All security audits are conducted in order to: ensure integrity, confidentiality, and availability of information and resources, to investigate possible security incidents and ensure conformance to GuidedChoice security policies, and to monitor user or system activity where appropriate. The Security Audit Policy allows for routine security checks to be implemented across all GuidedChoice networks, servers, computers, laptops, and mobile devices.

Our audits have revealed potential vulnerabilities in the past. For example, prior to 2002 we disclosed in Request for Proposals (RFP's) our hardware and software specifications at the request of prospective clients. A process audit revealed that by so doing, we could be making ourselves vulnerable to any weaknesses in the configurations known to hackers. We actually determined one



such weakness was the use of our UNIX operating system on a Sun Microsystems server. Since then, we have not disclosed any detailed data on our systems configurations to any outside firm, though we are continually pressured to do so by prospective clients. Annually, during our system security audits, low and medium risk issues are usually revealed, though no high-risk issues have been revealed. We have always been quick to fix any of the raised issues because our security procedure frequently checks the status of our system's protection.

## Risk Assessment

In addition the Manager of Security oversees our risk assessment team and the risk assessments (RAs) performed. According to our Risk Assessment Policy, GuidedChoice may conduct a RA on any entity within GuidedChoice or any outside entity that has signed a *Third Party Agreement* with GuidedChoice. The Risk Assessment has a three-step procedure to define the urgency level of a security issue and determine any areas of vulnerability in order to create the appropriate remediation. The following is the three-step protocol of a RA:

1. Commercial Vulnerability Product
  - a. GuidedChoice will maintain Commercial Vulnerability Assessment software and apply it every month. The results will be reviewed by the risk team and will assign an urgency level to each issue uncovered.
2. Every Vendor Notification
  - a. Whenever a security issue email notification is received, the risk team will assess the urgency level of the issue.
3. Security Issues Website
  - a. The security team will go to several industrial leading websites to keep updated on current vulnerabilities.

The risk assessments performed by our Manager of Security are extremely valuable to maintaining a clear view of our vulnerabilities. Another way we track any weaknesses is through our interactions with partners and security organizations. Our partners experience the latest breach attempts and can provide first hand



advice on how to combat those hacker techniques. Our security audits and risk assessments have assisted us in finding lower level vulnerabilities, however we believe it is far more effective to proactively keep abreast of the latest security breaches and corresponding corrective technologies.

### **An Evolving Protection Plan**

GuidedChoice has a variety of policies pertaining to router, server, internal labs, remote access, DMZ labs, anti-virus, dial-in access, email, network, and wireless communication security. Technology does not stop evolving; therefore our security needs to constantly be adapting to provide the best possible protection. A list of security policies is not the only layer of defense against data theft and or corruption.

Millions of security applications have been developed to support software and hardware security measures. GuidedChoice has specific security criteria that all software must meet before it is used on any of our devices, networks, or servers. The Manager of Security is also responsible for researching the best security applications to update all of GuidedChoice with the best protection available. GuidedChoice is currently available to over 4 million participants through our company clients. We would never risk their security by not properly maintaining ours.

There are many steps to providing the best security plan possible for all participants. Hiring a certified and knowledgeable Manager of Security is a crucial improvement companies can make to immediately improve their protection. A company's knowledge of vulnerability in their security is the first step in creating a solution to the problem. As technology changes so does security procedure; the Manager of Security should constantly be learning new ways to protect their company's classified data. Frequent recertification programs could be encouraged to maintain up to date security procedures. Lastly, companies should reevaluate the data they request from their current customers to ensure that they are only securing the confidential data necessary to perform their specific duty. The more PII they collect, the more security and encryption need to be implemented.



Thank you for taking the time to consider our security policy suggestions. It is our hope at GuidedChoice that companies will promote security procedures and policies that will evolve to prevent any further data breaches. In the appendix of this testimony is a copy of our Security Policy Table of Contents for any company to mirror when building their own security procedures and policy. As the counsel continues to discuss the security challenges posed by technology advancement we hope to provide an unbiased perspective of the best security options possible.

## Appendix

### Table of Contents

<b>GuidedChoice Ethics Policy</b> .....	<b>9</b>
<b>Overview</b> .....	<b>9</b>
<b>Purpose</b> .....	<b>9</b>
<b>Scope</b> .....	<b>9</b>
<b>Policy</b> .....	<b>9</b>
Executive Commitment to Ethics .....	9
Employee Commitment to Ethics.....	9
Company Awareness .....	10
Maintaining Ethical Practices.....	10
Unethical Behavior .....	10
Enforcement .....	10
<b>Information Sensitivity Policy</b> .....	<b>11</b>
<b>Purpose</b> .....	<b>11</b>
<b>Scope</b> .....	<b>11</b>
<b>Policy</b> .....	<b>12</b>
<b>Enforcement</b> .....	<b>14</b>
<b>Definitions</b> .....	<b>14</b>
<b>Terms and Definitions</b> .....	<b>14</b>
Appropriate measures .....	14
Configuration of GuidedChoice-to-other business connections .....	14
Delivered Direct; Signature Required .....	14
Approved Electronic File Transmission Methods.....	15
Envelops Stamped Confidential .....	15
Approved Electronic Mail .....	15
Approved Encrypted email and files.....	15
Company Information System Resources .....	15
Expunge .....	15
Individual Access Controls.....	15
Insecure Internet Links .....	15
Encryption.....	15
One Time Password Authentication .....	16
Physical Security.....	16
Private Link.....	16
<b>GuidedChoice’s Manager Of Security Acceptable Use Policy</b> .....	<b>16</b>
<b>1.0 Overview</b> .....	<b>16</b>
<b>2.0 Purpose</b> .....	<b>17</b>
<b>3.0 Scope</b> .....	<b>17</b>
<b>4.0 Policy</b> .....	<b>17</b>
4.1 General Use and Ownership.....	17
4.2 Security and Proprietary Information .....	18
4.3. Unacceptable Use.....	18
<b>5.0 Enforcement</b> .....	<b>20</b>

<b>6.0 Definitions</b> .....	<b>20</b>
<b>Risk Assessment Policy</b> .....	<b>21</b>
<b>1.0 Purpose</b> .....	<b>21</b>
<b>2.0 Scope</b> .....	<b>21</b>
<b>3.0 Policy</b> .....	<b>21</b>
<b>4.0 Risk Assessment Process</b> .....	<b>21</b>
Risk/Vulnerability Assessment.....	21
Urgency Level of Assessment.....	21
Learning About Vulnerabilities .....	24
<b>5.0 Enforcement</b> .....	<b>25</b>
<b>6.0 Definitions</b> .....	<b>25</b>
Terms Definitions.....	25
<b>Security Audit Policy</b> .....	<b>26</b>
<b>1.0 Purpose</b> .....	<b>26</b>
<b>2.0 Scope</b> .....	<b>26</b>
<b>3.0 Policy</b> .....	<b>26</b>
<b>4.0 Enforcement</b> .....	<b>26</b>
<b>Password Policy</b> .....	<b>27</b>
<b>1.0 Overview</b> .....	<b>27</b>
<b>2.0 Purpose</b> .....	<b>27</b>
<b>3.0 Scope</b> .....	<b>27</b>
<b>4.0 Policy</b> .....	<b>27</b>
4.1 General .....	27
4.2 Guidelines.....	28
<b>5.0 Enforcement</b> .....	<b>30</b>
<b>6.0 Definitions</b> .....	<b>30</b>
Terms & Definitions .....	30
<b>Router Security Policy</b> .....	<b>31</b>
<b>1.0 Purpose</b> .....	<b>31</b>
<b>2.0 Scope</b> .....	<b>31</b>
<b>3.0 Policy</b> .....	<b>31</b>
<b>4.0 Enforcement</b> .....	<b>32</b>
<b>5.0 Definitions</b> .....	<b>32</b>
Terms Definitions .....	32
<b>Server Security Policy</b> .....	<b>33</b>
<b>1.0 Purpose</b> .....	<b>33</b>
<b>2.0 Scope</b> .....	<b>33</b>
<b>3.0 Policy</b> .....	<b>33</b>
3.1 Ownership and Responsibilities .....	33
3.2 General Configuration Guidelines.....	33
3.3 Monitoring .....	34
3.4 Compliance .....	34
<b>4.0 Enforcement</b> .....	<b>35</b>
<b>5.0 Definitions</b> .....	<b>35</b>
Term: Definition.....	35

<b>Internal Lab Security Policy .....</b>	<b>36</b>
<b>1.0 Purpose.....</b>	<b>36</b>
<b>2.0 Scope.....</b>	<b>36</b>
<b>3.0 Policy .....</b>	<b>36</b>
3.1 Ownership Responsibilities .....	36
3.2 General Configuration Requirements .....	37
<b>4.0 Enforcement.....</b>	<b>38</b>
<b>Remote Access Policy.....</b>	<b>40</b>
<b>1.0 Purpose.....</b>	<b>40</b>
<b>2.0 Scope.....</b>	<b>40</b>
<b>3.0 Policy .....</b>	<b>40</b>
3.1 General .....	40
3.2 Requirements .....	41
<b>4.0 Enforcement.....</b>	<b>42</b>
<b>5.0 Definitions .....</b>	<b>42</b>
Term    Definition .....	42
<b>DMZ Lab Security Policy .....</b>	<b>44</b>
<b>1.0 Purpose.....</b>	<b>44</b>
<b>2.0 Scope.....</b>	<b>44</b>
<b>3.0 Policy .....</b>	<b>44</b>
3.1. Ownership and Responsibilities .....	44
3.2. General Configuration Requirements .....	45
<b>4.0 Enforcement.....</b>	<b>46</b>
<b>5.0 Definitions .....</b>	<b>46</b>
Terms    Definitions .....	46
<b>Internet DMZ Equipment Policy.....</b>	<b>48</b>
<b>1.0 Purpose.....</b>	<b>48</b>
<b>2.0 Scope.....</b>	<b>48</b>
<b>3.0 Policy .....</b>	<b>48</b>
3.1. Ownership and Responsibilities .....	48
3.2. General Configuration Policy.....	49
3.3. New Installations and Change Management Procedures.....	50
3.4. Equipment Outsourced to External Service Providers.....	50
<b>4.0 Enforcement.....</b>	<b>50</b>
<b>5.0 Definitions .....</b>	<b>51</b>
Terms    Definitions .....	51
<b>Lab Anti-Virus (Internet Security) Policy .....</b>	<b>52</b>
<b>1.0 Purpose.....</b>	<b>52</b>
<b>2.0 Scope.....</b>	<b>52</b>
<b>3.0 Policy .....</b>	<b>52</b>
<b>4.0 Enforcement.....</b>	<b>52</b>
<b>Extranet Policy.....</b>	<b>53</b>
<b>1.0 Purpose.....</b>	<b>53</b>
<b>2.0 Scope.....</b>	<b>53</b>
<b>3.0 Policy .....</b>	<b>53</b>

3.1 Pre-Requisites .....	53
3.2 Establishing Connectivity.....	54
3.3 Modifying or Changing Connectivity and Access .....	54
3.4 Terminating Access.....	54
<b>4.0 Enforcement.....</b>	<b>54</b>
<b>5.0 Definitions .....</b>	<b>55</b>
Terms    Definitions .....	55
<b>Application Service Providers (ASP) Policy .....</b>	<b>56</b>
<b>1.0 Purpose.....</b>	<b>56</b>
<b>2.0 Scope.....</b>	<b>56</b>
<b>3.0 Policy .....</b>	<b>56</b>
3.1 Requirements of Project Sponsoring Organization .....	56
3.2 Requirements of the Application Service Provider.....	56
<b>4.0 Enforcement.....</b>	<b>57</b>
<b>5.0 Definitions .....</b>	<b>57</b>
Terms    Definitions.....	57
<b>ASP Security Standards .....</b>	<b>58</b>
<b>1.0 Overview .....</b>	<b>58</b>
<b>2.0 Scope.....</b>	<b>58</b>
<b>3.0 Responding to These Standards.....</b>	<b>58</b>
<b>4.0 Standards.....</b>	<b>59</b>
4.1 General Security .....	59
4.2 Physical Security .....	59
4.3 Network Security.....	59
4.4 Host Security.....	60
4.5 Web Security.....	61
4.6 Cryptography.....	61
<b>DB Password Policy.....</b>	<b>62</b>
<b>1.0 Purpose.....</b>	<b>62</b>
<b>2.0 Scope.....</b>	<b>62</b>
<b>3.0 Policy .....</b>	<b>62</b>
3.1 General .....	62
3.2 Specific Requirements .....	62
3.3 Access to Database User Names and Passwords.....	63
3.4 Coding Techniques for implementing this policy .....	63
<b>4.0 Enforcement.....</b>	<b>63</b>
<b>5.0 Definitions .....</b>	<b>63</b>
Term    Definition .....	63
<b>Dial-In Access Policy .....</b>	<b>65</b>
<b>1.0 Purpose.....</b>	<b>65</b>
<b>2.0 Scope.....</b>	<b>65</b>
<b>3.0 Policy .....</b>	<b>65</b>
<b>4.0 Enforcement.....</b>	<b>65</b>
<b>Analog/ISDN Line Security Policy .....</b>	<b>66</b>
<b>1.0 Purpose.....</b>	<b>66</b>

<b>2.0 Scope</b> .....	<b>66</b>
<b>3.0 Policy</b> .....	<b>66</b>
3.1 Scenarios & Business Impact.....	66
3.2 Facsimile Machines .....	66
3.3 Computer-to-Analog Line Connections.....	67
3.4 Requesting an Analog/ISDN Line .....	67
<b>4.0 Enforcement</b> .....	<b>68</b>
<b>Acceptable Encryption Policy</b> .....	<b>69</b>
<b>1.0 Purpose</b> .....	<b>69</b>
<b>2.0 Scope</b> .....	<b>69</b>
<b>3.0 Policy</b> .....	<b>69</b>
<b>4.0 Enforcement</b> .....	<b>69</b>
<b>5.0 Definitions</b> .....	<b>69</b>
Term: Definition .....	69
<b>Email Retention Policy</b> .....	<b>70</b>
<b>1.0 Purpose</b> .....	<b>70</b>
<b>2.0 Scope</b> .....	<b>70</b>
<b>3.0 Policy</b> .....	<b>70</b>
3.1 Administrative Correspondence .....	70
3.2 Fiscal Correspondence .....	71
3.3 General Correspondence .....	71
3.4 Ephemeral Correspondence.....	71
3.5 Instant Messenger Correspondence.....	71
3.6 Encrypted Communications.....	71
3.7 Recovering Deleted Email via Backup Media .....	71
<b>4.0 Enforcement</b> .....	<b>71</b>
<b>5.0 Definitions</b> .....	<b>71</b>
Terms and Definitions.....	71
<b>Automatically Forwarded Email Policy</b> .....	<b>73</b>
<b>1.0 Purpose</b> .....	<b>73</b>
<b>2.0 Scope</b> .....	<b>73</b>
<b>3.0 Policy</b> .....	<b>73</b>
<b>4.0 Enforcement</b> .....	<b>73</b>
<b>5.0 Definitions</b> .....	<b>73</b>
Terms    Definitions.....	73
<b>Guidelines for Hardware Purchasing and Upgrades</b> .....	<b>75</b>
<b>1.0 Purpose</b> .....	<b>75</b>
<b>2.0 Scope</b> .....	<b>75</b>
<b>3.0 Policy</b> .....	<b>75</b>
3.1 Requirements .....	75
<b>4.0 Enforcement</b> .....	<b>75</b>
<b>Guideline for Software Purchasing and Upgrades</b> .....	<b>76</b>
<b>1.0 Purpose</b> .....	<b>76</b>
<b>2.0 Scope</b> .....	<b>76</b>
<b>3.0 Policy</b> .....	<b>76</b>

3.1 Requirements .....	76
<b>4.0 Enforcement.....</b>	<b>76</b>
<b>Backup and Recovery Policy .....</b>	<b>77</b>
<b>1.0 Purpose.....</b>	<b>77</b>
<b>2.0 Scope.....</b>	<b>77</b>
<b>3.0 Policy .....</b>	<b>77</b>
3.1 Requirements .....	77
3.2 Contingency and Recovery .....	77
<b>4.0 Enforcement.....</b>	<b>78</b>
<b>Internal Software Development.....</b>	<b>79</b>
<b>1.0 Purpose.....</b>	<b>79</b>
<b>2.0 Scope.....</b>	<b>79</b>
<b>3.0 Policy .....</b>	<b>79</b>
3.1 Requirements .....	79
<b>4.0 Enforcement.....</b>	<b>79</b>
<b>5.0 Access Controls .....</b>	<b>80</b>
<b>6.0 Policy .....</b>	<b>80</b>
<b>Guidelines on Anti-Virus Process .....</b>	<b>81</b>
<b>Acquisition Assessment Policy .....</b>	<b>82</b>
<b>1.0 Purpose.....</b>	<b>82</b>
<b>2.0 Scope.....</b>	<b>82</b>
<b>3.0 Policy .....</b>	<b>82</b>
I. General .....	82
II. Requirements .....	82
<b>4.0 Enforcement.....</b>	<b>83</b>
<b>5.0 Definitions .....</b>	<b>83</b>
<b>Virtual Private Network (VPN) Policy.....</b>	<b>84</b>
<b>1.0 Purpose.....</b>	<b>84</b>
<b>2.0 Scope.....</b>	<b>84</b>
<b>3.0 Policy .....</b>	<b>84</b>
<b>4.0 Enforcement.....</b>	<b>85</b>
<b>5.0 Definitions .....</b>	<b>85</b>
Term    Definition .....	85
<b>Wireless Communication Policy .....</b>	<b>86</b>
<b>1.0 Purpose.....</b>	<b>86</b>
<b>2.0 Scope.....</b>	<b>86</b>
<b>3.0 Policy .....</b>	<b>86</b>
3.1 Register Access Points and Cards .....	86
3.2 Approved Technology.....	86
3.3 VPN Encryption and Authentication .....	86
3.4 Setting the SSID .....	86
<b>4.0 Enforcement.....</b>	<b>87</b>
<b>5.0 Definitions .....</b>	<b>87</b>
Terms    Definitions.....	87

<b>GuidedChoice Third Party Connection Agreement .....</b>	<b>88</b>
<b>Third Party Connection Agreement— .....</b>	<b>89</b>
<b>Terms And Conditions.....</b>	<b>89</b>
<b>GuidedChoice-Owned Equipment.....</b>	<b>89</b>
<b>Network Connection Policy .....</b>	<b>92</b>
<b>A. Third-Party Connection Requests and Approvals.....</b>	<b>92</b>
<b>B. Connectivity Options .....</b>	<b>93</b>
<b>C. Third Party (Partner) Access Points .....</b>	<b>93</b>
<b>D. Services Provided.....</b>	<b>93</b>
<b>E. Authentication for Third Party Network Connections.....</b>	<b>94</b>
<b>F. GuidedChoice Equipment at Third Party Sites.....</b>	<b>95</b>
<b>G. Protection of Company Private Information and Resources .....</b>	<b>95</b>
<b>H. Audit and Review of Third Party Network Connections .....</b>	<b>96</b>
<b>I. GuidedChoice Corporate IT Information Security Organization .....</b>	<b>96</b>
<b>J. GuidedChoice Enterprise Network Services.....</b>	<b>96</b>
<b>Third Party Connection Request .....</b>	<b>97</b>
<b>Information Requirements Document .....</b>	<b>97</b>
<b>Incidence Response Plan .....</b>	<b>99</b>
<b>Purpose.....</b>	<b>99</b>
<b>Scope.....</b>	<b>99</b>
<b>Information Security Incident .....</b>	<b>99</b>
Classification: .....	99
<b>Response Process:.....</b>	<b>100</b>
<b>ISIRT Associate Members .....</b>	<b>103</b>