

10. **CONSENT AGENDA**

- c. Approval of an agreement with LarsonAllen to provide information technology consulting and advisory services in the amount of \$35,000 and authorize the City Manager to execute same AND **RESOLUTION 11-005 APPROVING BUDGET AMENDMENT/TRANSFER NO. 2011-006 AND PROVIDING AN EFFECTIVE DATE** (To transfer \$35,000 from the General Fund reserve for contingencies for LarsonAllen, LLP to provide information technology consulting and advisory services. This budget amendment does not increase or decrease the FY11 budget)

November 24, 2010

Mr. Bert Smith
City of Sanibel
800 Dunlop Road
Sanibel, FL 33957

Dear Mr. Smith:

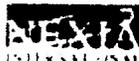
We are pleased you have considered us to provide you with information technology consulting and advisory services. This agreement has been prepared based on our understanding of your needs obtained in our previous discussions and correspondence. If this agreement is consistent with your understanding, you may accept it by signing in the space provided at the end of this document.

We understand our agreement to be as follows:

1. **Project Description.** LarsonAllen LLP (LarsonAllen) will conduct an Information Security Policy Review, an Information Technology Risk Assessment, External Network Penetration Testing, and an Internal Vulnerability Assessment as described in Addendum A. This engagement is not an assurance audit as defined by professional standards and should not be construed as such.
2. **Time for Performance.** We will start performing our services on a mutually agreeable schedule that will be determined upon contract acceptance.
3. **Compensation.** The itemized professional fees for the services as described in Addendum A are:

Information Security Policy Review.....	Hourly Estimate -	\$9,000
Information Technology Risk Assessment.....		\$9,000
External Network Penetration Testing.....		\$5,000
Internal Vulnerability Assessment.....		\$7,000
TOTAL ***		\$30,000

***The assistance LarsonAllen will provide to document a comprehensive set of information security policies will be billed at an hourly rate – all time will be billed. Based on the discussions we have had with the City of Sanibel, we estimate our fees to be \$9,000 (derived by an estimate of 45 hours at a rate of \$200/hour). If the City of Sanibel requests additional assistance that what was discussed, an hourly rate of \$200/hour will be utilized. All other fees noted above will be a fixed fee.



LarsonAllen LLP is a member of Nexia International,
a worldwide network of independent accounting and consulting firms.

These fees do not include travel time and reimbursable expenses (such as travel and lodging, if necessary) which will be billed separately. We will invoice you monthly for services rendered as well as for expenses and travel time incurred in connection with the project. Actual and reasonable expenses and travel time incurred will be invoiced at the actual expense. We will expect you to advise us promptly if you dispute any invoiced amount or if you believe there is a problem on the project, so that we can promptly resolve such matters.

4. Additional Services. If modifications or changes are required during the course of the project that is beyond the initial scope of services, or if you request that we perform any additional services, we will provide you with an Additional Services Authorization form for your signature. This form will advise you of the additional fee and any extra time required for such items to facilitate a clear understanding of the project status.
5. Our Responsibilities. We will exercise our best efforts to assess the current status of your network security and to protect you from both internal and external attacks on your information services network. Our audit of your network, however, will provide an assessment only as of the time of our analysis and we cannot guarantee protection against future penetration of your network caused by novel strategies or devices or due to the failure of you or your employees, agents or vendors to maintain your network or to adopt reasonable security precautions. We will perform our services as an independent consultant and will be responsible for the means and methods of providing our services. We will provide our services in a professional and workmanlike manner in accordance with generally accepted industry standards. LarsonAllen will not perform management functions or make management decisions on behalf of the City of Sanibel. However, we will provide advice and recommendations to assist management of the City of Sanibel in performing its functions and making decisions. Warranties on third-party software, services or equipment that we may employ on your behalf will be limited to the obligations of such third parties and we will pass any such warranties on to you. We will hold you harmless from any damages or liabilities resulting from third-party claims that any equipment or software we may employ on your behalf infringes U.S. patents, copyrights or similar intangible rights, provided that you promptly notify us of the matter, cooperate with us as requested, and permit us to control the investigation, defense and disposition of such matter. You shall otherwise be solely responsible for the accuracy and integrity of your own data, reports, documentation and security. EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION, NO WARRANTY OR ASSURANCE, EXPRESS, IMPLIED OR STATUTORY, IS GIVEN BY US WITH RESPECT TO SOFTWARE, SERVICES OR ANY OTHER MATTER, INCLUDING, WITHOUT LIMITATION (AND WE SPECIFICALLY DISCLAIM) ALL WARRANTIES OF TITLE, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. In no event shall we be liable, whether in contract or in tort or under any other legal theory (including, without limitation, strict liability and negligence) for lost profits or revenues, loss or interruption of use, lost or damaged data, reports, documentation or security, or similar economic loss, or for any indirect, special, incidental, consequential or similar damages, arising out of or in connection with the performance or non-performance of this agreement, or for any claim made against you by any other party, even if we have been advised of the possibility of such claim. In no event shall our liability under any claim exceed the total amount of fees paid to us relating to the services in question. No action, regardless of form, arising out of or in connection with this agreement may be brought more than one (1) year after the first to occur of (i) the termination or expiration of this agreement or (ii) the event giving rise to such cause of action.
6. Your Responsibilities. We will expect you to provide us with all necessary information regarding your information services network and your requirements for the project in sufficient time to allow us to adhere to the project schedule. You are responsible for management decisions and

functions. We will expect you to designate a competent project representative who will oversee these services and be fully authorized to make decisions on your behalf and to authorize timely payment of our invoices. You are responsible for evaluating the adequacy and results of the services performed and accepting responsibility for the results. We will expect you to adopt such reasonable network security measures as we, or other security consultants may recommend in order to minimize potential breaches of your network security. You are also responsible for establishing and maintaining internal controls, including monitoring ongoing activities.

7. Payment for Employment of Our Personnel. In the event that you employ one of our professional employees during the performance of the project or within one year after it has been completed, in order to compensate us for lost benefits and the cost of locating and training a replacement you agree to pay us a sum equal to fifty percent of the annual salary you pay to the employee during the first year of employment.
8. Subcontractors. LarsonAllen may, at times, use subcontractors to perform services under this agreement and they may have access to your information and records. Any such subcontractors will be subject to the same restrictions on the use of such information and records as apply to LarsonAllen under this agreement. LarsonAllen will be as responsible for any act done by these subcontractors as it is for its personnel under this agreement.
9. Insurance. During the course of the project, we will maintain the statutory workers' compensation and employer's liability insurance required by law, as well as adequate comprehensive general liability and professional liability insurance.
10. Ownership of Documents. All materials and automated files that we bring into the engagement will remain our property. Any such items created for you during the project shall become your property to be used solely for your internal purposes. You agree not to reproduce such items for distribution or disclose their contents to third parties. We will expect you to indemnify us for any claims arising out of the improper re-use of such items, including, but not limited to, any claims arising out of their re-use for additional projects having different requirements or arising out of claims from third parties to whom you have given such items.
11. Suspension and Termination. We reserve the right to suspend work if we are not paid for our services in a timely manner. Either of us may terminate this agreement for failure of the other to fulfill its obligations. You may also terminate this agreement if you decide to discontinue the project, by giving us seven days written notice. In such case, we will be entitled to compensation for services rendered and costs incurred up to that time.
12. Assignment. Neither of us may assign our rights under this agreement without the other's prior written consent.
13. Governing Law. This Agreement shall be governed and construed in all respects in accordance with the laws of the State of Florida as they apply to a contract entered into and performed in that state.
14. Mediation. All Disputes between us shall first be submitted to non-binding mediation by written notice ("Mediation Notice") to the other party. In mediation, we will work with you to resolve any differences voluntarily with the aid of an impartial mediator. The mediator will be selected by mutual agreement, but if we cannot agree on a mediator, one shall be designated by the American Arbitration Association ("AAA").

The mediation will be conducted as specified by the mediator and agreed upon by the parties. The parties agree to discuss their differences in good faith and to attempt, with the assistance of the mediator, to reach an amicable resolution of the Dispute.

Each party will bear its own costs in the mediation. The fees and expenses of the mediator will be shared equally by the parties.

15. Limitation of Remedies. Our role is strictly limited to the engagement described in this letter, and we offer no assurance as to the results or ultimate outcomes of this engagement or of any decisions that you may make based upon our communications or our reports to you. You will be solely responsible for making all decisions concerning the contents of our communications and reports, for the adoption of any plans and for implementing any plans you may develop, including any that we may discuss with you.

You agree that it is appropriate to limit the liability of LarsonAllen, its principals, directors, officers, employees and agents ("we" or "us") and that this limitation of remedies provision is governed by the laws of the State of Florida, without giving effect to choice of law principles.

The exclusive remedy available to you shall be the right to pursue claims for actual damages that are directly caused by acts or omissions that are breaches by us of our duties under this agreement, but any recovery on any such claims, including any costs and attorneys' fees incurred in pursuing them, shall not exceed \$300,000.

16. Entire Agreement; No Oral Modification. This agreement, and any attached exhibits or schedules, constitutes our full and complete agreement. It supersedes and replaces any and all previous representations, understandings and agreements, written or oral, relating to the project. There shall be no oral modification of this agreement, as it may not be modified or changed except in writing signed by both parties.

If the foregoing accurately reflects our understanding, please indicate your agreement by signing this letter in the space provided below and returning it to us. We look forward to a successful completion of the project.

LarsonAllen LLP



Randall J. Romes, CISSP, CRISC, MCP
Principal

Accepted by the City of Sanibel

By: _____
Print Name: _____
Title: _____
Date: _____

APPROVED AS TO FORM:



CITY ATTORNEY



APPROVED FINANCIAL SUPERVISOR
Sarah A. Edwards, Finance Director

This document is proprietary to LarsonAllen LLP. The information contained in this document may not be duplicated, disclosed, or used other than for evaluation purposes.

Addendum A – Scope of Services

Information Security Policy Review and Development

Overview	Organizations should document a comprehensive set of information security policies to provide governance around the IT environment of an organization.
Objective	Our objective is to assist with the development of a comprehensive set of information security policy documents that cover all functional areas and sub-areas within the IT environment.
Approach	<p>To satisfy the project objective, LarsonAllen will approach the project as follows:</p> <ol style="list-style-type: none">1. Obtain all IT policies that currently exist within the organization and review for appropriateness.2. Provide a comprehensive set of policy templates to management and discuss each policy and the content that is required to be documented in each policy.3. Review policy documents once completed by the City of Sanibel and provide comments and feedback. The City of Sanibel has communicated that they would like to document the policies themselves with oversight from LarsonAllen.4. Finalize policy documents.
Deliverable	At the conclusion of the policy review and development process, the City of Sanibel will have a comprehensive set of information security policies to be utilized by the organization.

Risk Assessment of Information Technology Environment

Overview	Organizations should perform an annual risk assessment of the information technology environment to ensure inherent and specific risks to the organization are identified and addressed appropriately and timely.
Objective	Our objective is to provide the City of Sanibel with a validated risk assessment of their technology environment. The results of the risk assessment will provide the City of Sanibel with the opportunity to develop and implement mitigating administrative, technical, and physical controls to minimize the possibility of adverse events that may occur. The results will also assist in providing the City of Sanibel an assessment of what areas appear to be of highest risk to allow the organization the opportunity to address risks based on priority.
Approach	<p>To satisfy the project objective, LarsonAllen will approach the project as follows:</p> <ol style="list-style-type: none">1. Obtain an organization chart to illustrate the roles and reporting hierarchy that will impact the risk assessment process.2. Request the City of Sanibel to complete a profile document with a description of the current technical infrastructure, including application systems and support services.3. Define and create the risk universe and risk model, identify risk ranking criteria definitions (impact and vulnerability), and agree on a measureable scale and deliverable format.4. Interview designated personnel identified within the scope of the project to review IT security processes and discuss inherent and specific risks within the IT environment.5. Document and summarize interview results and perform initial ranking of risks identified based on our current understanding.6. Review risks and recommendations with the City of Sanibel to validate the information gathered during the risk assessment process are accurate.7. Finalize the results and the risk assessment report. The outcome of the assessment will identify the inherent risks and specific risks identified within the IT environment.8. Present the preliminary report to management for review with the opportunity to validate the content and make appropriate changes prior to finalization.
Deliverable	At the conclusion of the risk assessment process, the City of Sanibel will receive a validated risk assessment report that addresses risks related to administrative, technical, and physical areas.

External Network Penetration Testing

Overview	The External Network Penetration Test is designed to aggressively test your network perimeter to identify exposure to security breaches from outside your network. Completeness is a critical objective when securing the network perimeter; therefore, our testing approach is designed to search your entire infrastructure to identify rogue gateway entry points, including internet, VPN, dial-up, wireless, etc.
Objective	Our objective is to identify potential vulnerabilities outside the network that might be used to: <ul style="list-style-type: none">• Gain unauthorized access to sensitive confidential information.• Modify or destroy data.• Operate trusted business systems for non-business purposes.
Approach	<p>To satisfy the project objective, LarsonAllen will use a variety of manual and automated tools to test the configuration of all internet gateway connections. Our testing will identify and test all such gateway connections in place on your current network configuration. We will then obtain appropriate documentation to verify that our activity was properly detected and logged.</p> <p>The complete network penetration test occurs in four very distinct phases:</p> <p><u>Phase 1 – Footprinting</u></p> <p>Footprinting identifies all internet points of presence (potential entry points). In this phase, completeness is critical - all entry points need to be identified and tested.</p> <p><u>Phase 2 – Enumeration</u></p> <p>All hosts identified in the footprinting stage are analyzed to determine:</p> <ul style="list-style-type: none">• Type of host (i.e. router, firewall, web server, etc.).• Operating system in use (including version and patch level).• Services available and listening. <p><u>Phase 3 – Automated Scanning</u></p> <p>Nessus and other automated scanning tools are used to determine potential vulnerabilities available to be exploited. Information used in the footprinting and enumeration stage is used to “tune” the scanner to focus its effort, improve its feedback, and eliminate unnecessary scanning.</p> <p><u>Phase 4 – Analysis and Penetration</u></p> <p>This phase typically represents 85% of our level of effort in a penetration test. We analyze the results of the first three phases to prepare a hacking plan. We verify the results of the automated scanning to ensure that we do not present “false positives” in our report. We perform numerous manual tests that cannot be accomplished with automated scanning techniques. If we are “successful” in breaching your perimeter defense, we will quantify the extent of exposure in order to accomplish our critical objective of completeness.</p> <p>We perform a penetration test in the same way a malicious hacker will exploit your network. This is accomplished by not only performing a basic vulnerability scan but by also analyzing the results of the scan and building a plan of attack. Simple</p>

vulnerability scans cannot apply intelligence to the task of finding chains of risks and vulnerabilities on disparate systems that can be used to compromise the network. They often reveal numerous "low risk" vulnerabilities disclosed within the automated reports that commercial scanning tools produce. However, these "low risk" vulnerabilities can sometimes be used in concert, like piecing together a jigsaw puzzle, to produce a plan of attack that can create "very high risk" results.

Very often, we are successful in putting together a plan of attack that can result in root or administrator level compromise of every host on the client's network through a firewall, even though the initial scan results listed only low or medium risk vulnerabilities.

Our service verifies the results of the scan so your people do not have to chase false positives often caused by many scanning tools. This eliminates the need for your IT personnel to devote time and effort to this process.

For each vulnerability, or perhaps more importantly for each chain of vulnerabilities, we do our homework and present a best practice set of solutions. Sometimes a simple patch download will suffice, but more often than not, the solution is more complex.

Our developers keep us on the cutting edge. They are constantly producing proprietary tools to test for the presence of emerging vulnerabilities, often before tools such as Nessus have scripts available to test for them. An excellent example is the latest Internet Explorer vulnerabilities, which were tested by our group months before they were published.

We test for latest attacks, including so-called "Phishing" and "spear-Phishing" attacks, as well as web-based application vulnerabilities. Our network penetration test will include Phishing attempts, meant to test both the administrative and technical aspects of these dangerous and rapidly increasing threats. Our security auditors have the expertise to test for the presence of known and unknown vulnerabilities in web-based applications, including buffer overflows, cross-site scripting attacks, and SQL injection. Our developers and security auditors have discovered and documented the presence of previously unknown vulnerabilities in numerous on-line banking, e-commerce, and vendor supplied web-based administrative applications.

Deliverable

Our deliverable report will provide your network administrators with detailed recommendations for how to address specific findings. Successive tests will include findings in a table format that track remediation of previous findings, and identification of new risks.

Internal Vulnerability Assessment

Overview The Internal Vulnerability Assessment will be a technical evaluation of the key devices (i.e. file servers, mail servers, production servers, routers, switches, etc.) that reside on your trusted business network.

The Computer Security Institute estimates that only 3% of organizations have the appropriate security patches and configurations in place to protect their network from an internal breach or a successful perimeter breach. The internal vulnerability assessment is designed to confirm that your network is reasonably protected from these types of threats, which can be more disruptive and more expensive.

Objective Our objective is to identify potential vulnerabilities inside the network that might be used to:

- Gain unauthorized access to sensitive confidential information.
- Modify or destroy data.
- Operate trusted business systems for non-business purposes.

Approach The Internal Vulnerability Assessment occurs in two distinct phases:

Phase 1 - Internal Penetration Testing

Beginning with very limited privileges, (typically only a data port connection in a conference room) LarsonAllen will use automated and manual techniques to identify all significant network hosts and routing devices. We will then review their configuration using a combination of automated tools and manual information security checklists (i.e. hardening checklists). The Internal Penetration Testing includes the following:

- Identify live hosts and services available on the network.
- Perform automated vulnerability assessments using up-to-date open source and custom developed proprietary tools.
- Manual testing of the results from automated scan to eliminate false positives
- Exploit vulnerabilities to demonstrate possible privilege escalation scenarios.

Phase 2 - Configuration Audit and Process Review

During the configuration audit we will review key systems and processes to document current configurations:

- Perform service pack/security patch/hot-fix scanning to identify currently level up update on key systems on the network (MS Windows operating systems, UNIX systems, Novell systems, etc.).
- Configuration audits of key servers and routing devices against industry standard benchmarks.
- User account and password auditing to ensure compliance with information security policies.
- Review configuration of user account and group policy and auditing settings with Active Directory.
- Review configuration of 3rd party vendor installed/maintained systems.
- Review network/system security architecture.

- Review and vulnerability testing of VoIP communication infrastructure.
- Network traffic and packet capture analysis to determine if confidential information is transmitted in an unsecured manner.

Deliverable

Our deliverable report will provide your network administrators with detailed recommendations for how to address specific findings. Your network will be secured (hardened) from the inside to protect against malicious insiders, intruders who may gain physical access to network resources, or external hackers who successfully breach perimeter defenses.

RESOLUTION 11-005

APPROVING BUDGET AMENDMENT/TRANSFER NO. 2011-006 AND PROVIDING AN EFFECTIVE DATE

NOW, THEREFORE, BE IT RESOLVED by City Council of the City of Sanibel, Florida:

SECTION 1. The revised General Fund for fiscal year 2010-2011, Budget Amendment/Transfer BA 2011-006 true copy of which is attached hereto as Exhibit A and incorporated herein by this reference, is hereby approved and accepted.

SECTION 2. Effective date.

This resolution shall take effect immediately upon adoption.

DULY PASSED AND ENACTED by the Council of the City of Sanibel, Florida this 1st day of March, 2011.

AUTHENTICATION:

Kevin Ruane, Mayor

Pamela Smith, City Clerk

APPROVED AS TO FORM:

Kenneth B. Cuyler 2/9/11
Kenneth B. Cuyler, City Attorney Date

Vote of Councilmembers:

Ruane _____
Denham _____
Harrity _____
Jennings _____
Pappas _____

Date filed with City Clerk: _____

