OES SECURITY POLICY

Below is a copy of the security policy (short-form and long-form overview) that each user will see and be required to agree with before accessing the OES.

1.0 Security Policy Short-Form Overview (Sign-in Page)

You are accessing the Odysseus Enterprise System (OES) utilizing the Odysseus™ web-based preparedness and planning system developed and maintained by Integrated Solutions Consulting (ISC) and our clients. The OES program and system are the property of Integrated Solutions Consulting (ISC). The planning information (non-proprietary e.g. code and operational concepts) is the property of each client and ISC; the data is mutually protected as confidential. ISC will not share or disseminate any information developed by the client without the client's approval. The client will not share or disseminate any data developed by ISC without ISC's approval. Since the OES integrates client and ISC planning information, data, and concepts the OES security policy is designed to protect both parties as a collaborative endeavor.

By using OES, you consent to the terms set forth in this notice, the Security Policy, the Authorized User Agreement, the Access and Use Policy, and the Security Agreement. Access to OES is restricted to authorized users only. Unauthorized access, use, or modification of this system or of data contained herein, or in transit to/from this system, is strictly prohibited. Anyone who accesses OES without authorization or exceeds access authority, or obtains, alters, damages, destroys, or discloses information, or prevents authorized use of information on OES, may be subject to internal disciplinary action, may lose access to the system, and in serious cases make face further legal action.

By using OES you consent to monitoring of your access and use of the system and are advised that, if such monitoring reveals any violation of the Client and Security Policy, the Authorized User Agreement, the Access and Use Policy, the Security Agreement, or any other Terms of Use, the violation shall be reported to the proper supervisory personnel and may result in internal disciplinary action, loss of access to the system, and in serious cases further legal action. OES and any related equipment are subject to monitoring for administrative oversight, data security, and integrity, inquiries into alleged wrongdoing or misuse, to ensure proper performance of applicable security features and procedures, and in serious instances of abuse, may be used for law enforcement and/or criminal investigative purposes.

Social Security Number (SSN) and Health Insurance Portability and Accountability Act (HIPAA) information is not a component of the OES.

2.0 Security Policy Long-Form Overview

OES is protected through multiple security procedures and policies. The security procedures and policies are mutually reinforcing, and provide ISC, its Contractors, Trusted Partners, other Departments, and OES protection against unauthorized access to, misuse of, or infringement upon, Confidential and Proprietary Information.

ISC is facing many of the same issues that other emergency response agencies across the nation are facing. Information, tactical and strategic intelligence, and planning materials must be disseminated to increase operational effectiveness while maintaining an appropriate level of

security. OES is designed to balance these competing concerns, and every Authorized User has the obligation to maintain the policies contained in this agreement. To that end:

- Authorized Users must consider OES – both the software and the information contained therein – to be confidential and proprietary. Information may not be copied, downloaded, reproduced, captured, printed, distributed, divulged, published, or modified in any manner inconsistent with this Security Policy and/or in any way detrimental to Integrated Solutions Consulting (ISC). A definition of the components and information that constitute OES, and which must be protected under this Security Policy, can be found within the **Security Policy Definitions**. The definitions of Confidential Information and Proprietary Information can also be found within the **Security Policy Definitions** section.
- The information contained in OES is For Official Use Only (FOUO) and contains information that is exempt from public release under the Federal Freedom of Information Act (5 U.S.C. §552(b)) and the Illinois Freedom of Information Act (5 ILCS 140/7(1)(jj)), unless otherwise directed by the Executive Director of ISC or the Executive Director's designee(s). The Illinois Freedom of Information Act "exempts information contained in local emergency plans submitted in accordance with a local emergency plan ordinance." For more detail please review the **State of Illinois Attorney General's Office: A Guide to the Illinois Freedom of Information Act.**
- Authorized Users are responsible for protecting the information in OES. By providing his/her username and password during the login procedure, an Authorized User acknowledges his/her obligation under and agrees to the information security statements contained in, this Security Policy.
- Authorized users are required to use the industry-standard user name and password authentication to access OES. This ensures that access to OES is restricted to ISC personnel, Trusted Partners, Departments, and Contractors consistent with the terms of this Security Policy.
- Authorized Users are required to abide by the **Access and Use Policy** contained within this Security Policy. All of the information contained within OES, including Confidential and Proprietary Information, is restricted by Security Level. Authorized Users may not allow others to access or use any portion of OES beyond or outside of the others' Security Level. Similarly, Authorized Users are prohibited from viewing, accessing, or using any information, data, or other material in any portion of OES that the Authorized User knows or has reason to know is outside of his/her own Security Level or other clearance.

3.0 Security Policy Definitions

3.1 Authorized Agent

An "Authorized Agent" is an entity that has been granted a limited license to access and make professional use of OES consistent with the Authorized User's Security Level, professional responsibilities, and for the sole benefit of ISC. This limited license to access and make professional use of OES expressly forbids any user from copying, downloading, reproducing, capturing distributing, modifying, printing, divulging, publishing, or otherwise exploiting OES, or any portion thereof, without the express written permission of ISC, in any way inconsistent with

the terms of this Security Policy, and/or in any way that is detrimental to ownership, rights, interests, management, or control of OES by ISC. More information may be found in the Authorized User Agreement.

3.2 Authorized User

An "Authorized User" is: (1) any employee or agent of ISC (2) a Department, a Trusted Partner, a Contractor, or the employee or agent of a Department, a Trusted Partner, or a Contractor, or (3) any other person who, at the sole discretion of a OES Super-Administrator, is granted a limited license to access and use OES consistent with the terms of this Security Policy.

Each Authorized User is granted a limited license to access and make professional use of OES consistent with the Authorized User's Security Level, professional responsibilities, and for the sole benefit of ISC. This limited license to access and make professional use of OES expressly forbids any user from copying, downloading, reproducing, capturing distributing, modifying, printing, divulging, publishing, or otherwise exploiting OES, or any portion thereof, without the express written permission of ISC, in any way inconsistent with the terms of this Security Policy, and/or in any way that is detrimental to ownership, rights, interests, management, or control of OES by ISC. More information may be found in the Authorized User Agreement.

3.3 OES

"OES" consists of all documents, information, data, computer programs, software, source code, graphics, photographs, logos, textual materials, inventions, improvements, manuals and packaging, formulas, algorithms, logic, functionality, processes, trade secrets, trademarks, copyrights and copyrighted materials, electronic codes, mask works, innovations, patents, patent applications, discoveries, know-how, formats, test results, other research, maps, schematics, architectural drawings, plans, policies, and any other materials which comprise the computer software, web application, website, and all of the information and data, in whole or in part, contained therein (collectively the "Information"), created by and/or for ISC and implemented for ISC.

3.4 Confidential Information

"Confidential Information," as it pertains to ISC, is all Proprietary Information not generally known outside of ISC, as well as all Proprietary Information so known only through improper means.

3.5 Contractor

A "Contractor" is any business entity or person, whether for profit or not for profit, which is not a municipal corporation, local government agency, division or agency of any state government, the federal government, or any other governmental agency, which has been retained by or for ISC, a Department, a Trusted Partner, or another Contractor (e.g. where there is a contractor–subcontractor relationship) to provide goods or services to ISC. A Contractor and its agents or employees may be granted a limited license to access and make professional use of OES consistent with terms of this Security Policy at the sole discretion of an OES Super-Administrator.

3.6 Department

A "Department" is any department, agency, formal unit, or other subdivision of ISC. A Department and its agents or employees may be granted a limited license to access and make professional use of OES consistent with terms of this Security Policy at the sole discretion of an OES Super-Administrator.

3.7 For Official Use Only

"For Official Use Only" means use of OES, or Information contained therein, in a manner consistent with an Authorized User's Security Level, job responsibilities, and for the sole benefit of ISC.

3.8 Proprietary Information

"Proprietary Information" is all information and any idea in whatever form, tangible or intangible, pertaining in any manner to the software, systems, and Information provided by, or the business of, ISC, or its employees, clients, consultants, or business associates, which was produced by any employee or consultant of ISC in the course of his or her employment or consulting relationship or otherwise produced or acquired by or on behalf of ISC. By example and without limiting the foregoing definition, Proprietary Information shall include, but not be limited to:

3.8.1 formulas, algorithms, logic, functionality, research and development techniques, processes, trade secrets (including as defined in 765 ILCS 1065/2(d)), computer programs, software, electronic codes, mask works, inventions, innovations, patents, patent applications, discoveries, improvements, data, know-how, formats, test results, and research projects;

3.8.2 information about costs, profits, markets, sales, contracts and lists of customers, and distributors;

3.8.3 business, marketing, and strategic plans;

3.8.4 forecasts, unpublished financial information, budgets, projections, and customer identities, characteristics, and agreements;

3.8.5 employee personnel files and compensation information; and

3.8.6 information subject to trade secret, patent, copyright, or trademark protection consistent with applicable federal and state laws.

Proprietary Information is to be broadly defined and includes all information that has or could have commercial value or other utility in the business in which ISC is engaged or contemplates engaging, and all information of which the unauthorized disclosure could be detrimental to the interests of ISC, whether or not such information is identified as Proprietary Information by ISC.

3.9 Security Level

A "Security Level" defines the Information contained in OES to which an Authorized User will have access. An Authorized User's Security Level shall be determined by, or at the discretion of ISC, using a variety of criteria, including the user's rank or position, the purpose for requesting access to OES, responsibilities to ISC (and to his/her employer where it is an entity other than

ISC), experience, and other factors identified by, and applied in the sole discretion of, OES Super-Administrator(s).

3.10 Security Policy

The "Security Policy" consists of all terms, agreements, policies, and other language contained within this series of agreements, including but not limited to, all terms and conditions contained in Sections 1.0 through 9.8, identified as the Security Policy Definitions, Authorized User Agreement, Access and Use Policy, Security Agreement, Record of Distribution, Disclaimers, Miscellaneous Provisions, and the Short and Long Form Security Policy Overviews.

3.11 Super-Administrator

A "Super Administrator" is an Authorized User of OES with the highest-level security clearance allowed within OES software. A Super administrator may be an employee or agent of ISC and must complete separate confidentiality and protection of trade secret agreement.

3.12 Trusted Partner

A "Trusted Partner" is any agency, department, formal unit, other subdivision, or any agent or employee of any agency, department, formal unit, or other subdivision, of any municipal, local, state, or federal government body which works with ISC, but is not a part or subdivision of ISC.

4.0 Authorized User Agreement

Each Authorized User is granted a limited license to access and make professional use of OES consistent with the Authorized User's Security Level, professional responsibilities, and for the sole benefit of ISC. This limited license to access and make professional use of OES expressly forbids copying, downloading, reproducing, distributing, modifying, printing, divulging, publishing, or otherwise exploiting OES, or any portion thereof, without the express written permission of ISC, in any way inconsistent with the terms of this Security Policy, and/or in any way that is detrimental to ownership, rights, interests, management, or control of OES by ISC. No part of the electronic content, operational processes, and system design may be reproduced, stored in retrieval systems, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, in any manner inconsistent with this Security Policy, without prior written permission of ISC.

By accessing, viewing, contributing to, or otherwise using OES, an Authorized User agrees to be bound by, and to abide by, all of the policies included within this Security Policy. The limited license granted to an Authorized User under this Security Policy creates an affirmative duty on the part of each Authorized User to safeguard the Information, software, and other systems which constitute OES. An Authorized User agrees not to, directly or indirectly, use, make available, sell, disclose, or otherwise communicate to any third party, other than in his/her assigned duties and for the benefit of ISC, any Confidential or Proprietary Information during or after the term of this license.

The Authorized User agrees and warrants that the registration information submitted to ISC during the registration process is complete and accurate. The submission of any false or inaccurate information in connection with an OES user account constitutes a breach of the limited license granted under this Security Policy, and may, at the sole discretion of ISC, result in the immediate termination of the limited license to use and access OES.

5.0 Access and Use Policy

Authorized Users may access and use OES consistent with the terms contained within this Security Policy, and for the sole benefit of ISC. Use of OES under the limited license granted under this Security Policy is limited to use for internal business purposes and for no other purpose. Use of the limited license granted to each Authorized User (i.e. the user's "OES account") by anyone other than the Authorized User or for any purpose other than official use is prohibited. Authorized Users shall not share or permit access to their user names or passwords with or by any other person or entity, including, without limitation, any other person who may be employed by the Authorized User. Each employee, agent, or person within ISC, a Department, Trusted Partner, or Contractor must be individually registered and licensed to use OES.

Each Authorized User agrees, consistent with the restrictions listed in the Authorized User Agreement not to copy, download, reproduce, distribute, modify, print, divulge, publish, or otherwise use or exploit OES, or any portion thereof, without the express written permission of ISC, in any way inconsistent with the terms of this Security Policy, and/or in any way that is detrimental to ownership, rights, interests, management, or control of OES by ISC.

Each Authorized User agrees to notify ISC of any known or suspected unauthorized use(s) of OES, or any known or suspected breach of security, including loss, theft, or unauthorized disclosure of a password. The Authorized User shall be responsible for maintaining the confidentiality of his/her password. Any fraudulent, abusive, or otherwise illegal activity shall be grounds for termination of the limited license granted under this Security Policy.

The ISC Executive Director has delegated the responsibility of assigning the appropriate Security Level for Authorized Users of OES to the Department/Organization OES Liaison assigned to work with ISC in establishing OES security levels. The OES Liaison and authorized representative(s) will work collaboratively with ISC service unit managers, strike-team leaders, unit leaders, as well as other Departments, Trusted Partners, and Contractors, to optimally assign at its sole discretion the appropriate Security Level to each Authorized User. The OES Liaison has the authority to revoke access under the limited license or to change the Security Level of an Authorized User at any time for any reason.

Security Levels are established through system Security Roles and Workgroups. The OES Liaison and ISC will collaborate to create Security Roles and Workgroups that complement the

organizational structure of the Department. These Security Levels will grant privileges for user to read, edit, publish, and receive comments for specific chapters or sections within the OES. The OES Liaison is ultimately responsible for assigning the OES users into these Security Levels and maintaining a level of security integrity that corresponds to the sensitive nature of the content contained in the OES.

Independent of the security roles and workgroups maintained in the OES, a limited number of ISC and Department personnel will be given administrative rights to the OES. The OES Liaison is responsible for limiting the number of Department users being granted administrative access. There are two administration levels responsible for maintaining the overall OES system:

- **User Admin:** A User Administrator is the highest level of access granted within an instance. This administrator can create, edit, and maintain users within the OES including security rights and granting administrative privileges.
- **Data Admin:** A Data Administrator is responsible for maintaining the site and OES structure. This administrator can change the OES structure and site options and can change security privileges for Security Roles and Workgroups but cannot access information or options pertaining to individual users.

6.0 Security Agreement

This Security Agreement, in combination with the Authorized User Agreement, is designed to protect the Information of ISC, and the systems and other components contained within OES. The Authorized Agent will share and disseminate certain Information in OES to public, private, and nonprofit agencies, and partners from time to time. Accordingly, ISC has developed legal, operational, and technological protections to help ensure it controls the dissemination of appropriate information and protects ISC's operationally sensitive information within OES.

6.1 Ownership of Confidential and Proprietary Information; User's Duties

The Information contained within OES is owned exclusively by ISC. The content specifically concerning OES and its operations is the sole property of ISC. The multi- agency and All-Hazard content specifically developed by ISC is the sole property of ISC. ISC has agreed to not to disseminate or re-use with another client, and to protect, information concerning, and/or owned by Authorized Agent. Authorized Agent has agreed not to disseminate to any third party and protect information that is the sole property of ISC.

Further, ISC has developed and compiled, and will develop and compile, certain trade secrets, proprietary techniques and other Confidential and Proprietary Information which has great value to ISC's business. Portions of this Proprietary Information may be disclosed by or to Authorized Agent, its employees, agents, or other Personnel, Departments, Trusted Partners, and Contractors, and may include information developed or learned by an Authorized User during

the term of his/her limited license. Accordingly, Authorized Users have an affirmative duty to protect and keep confidential any and all Information viewed, accessed, learned, or otherwise obtained via use of OES, and to only disclose Information in a manner consistent with this Security Agreement, the Security Policy, and as expressly directed by ISC, for the sole benefit of ISC.

Authorized Users agree not to, directly or indirectly, use, make available, sell, disclose or otherwise communicate to any third party, other than in his/her assigned duties and for the benefit of ISC, and consistent with the terms of this Security Agreement, any of the ISC Confidential or Proprietary Information, either during or after the Authorized User's relationship with ISC. The Authorized User agrees not to publish, disclose or otherwise disseminate such information without the prior written approval of ISC. The Authorized User acknowledges that he/she is aware that the unauthorized disclosure of Confidential Information of ISC may be highly prejudicial to its interests, an invasion of privacy, and an improper disclosure of trade secrets.

6.2 Delivery of Confidential and Proprietary Information

Upon request, or when the Authorized User's relationship with ISC, a Department, Trusted Partner, or Contractor terminates, the Authorized User will immediately deliver to ISC all copies of any and all materials and writings received from, created for, or belonging to ISC, including, but not limited to, those which relate to or contain Confidential or Proprietary Information.

6.3 Location and Reproduction

The Authorized User shall maintain at his/her workplace or other location only such Confidential and/or Proprietary Information as he/she has a current "need to know." The Authorized User shall return to the appropriate person or location or otherwise properly dispose of Confidential and/or Proprietary Information once that need to know no longer exists. The Authorized User shall not make copies of or otherwise reproduce Confidential or Proprietary Information unless there is a legitimate business need of ISC for reproduction.

6.4 Prior Acts and Knowledge

The Authorized User represents and warrants that from the time of his/her first contact with ISC he/she has held in strict confidence all Confidential and Proprietary Information and has not disclosed any Confidential or Proprietary Information, directly or indirectly, to anyone outside the Department, or used, copied, published, or summarized any Confidential information, except to the extent otherwise permitted in this Agreement.

6.5 Third Party Information

The Authorized User acknowledges that the Authorized Agent has received, and in the future

will receive, from third parties certain confidential information subject to a duty on Authorized Agent's part to maintain the confidentiality of such information and to use it only for certain limited purposes. The Authorized User agrees that he/she will at all times hold all such confidential information in the strictest confidence and not to disclose or use it, except as necessary to perform his/her obligations to ISC and/or his/her employer in a manner consistent with ISC's agreement with such third parties. The Authorized User further agrees that he/she will execute all other and additional documents which any third-party may require covering the treatment of its confidential information before access to such information will be granted under the terms of this limited license.

6.6 Third Party Conflict Warranty

The Authorized User warrants and represents that his/her relationship with ISC does not and will not breach any agreements with or duties to a current or former employer, or any other third party. The Authorized User will not disclose or use on its behalf any confidential information belonging to others to which Authorized Agent does not have permission to use, and will not bring onto the premises of Authorized Agent, or use in OES, any confidential information belonging to any such party unless consented to in writing by such party or otherwise permitted by law.

6.7 Property Rights, Inventions, and New Ideas

The Authorized User agrees that any Subject Ideas or Inventions which he creates or helps to create, in whole or in part, through use of OES, or by use of information within OES, will be the property of ISC, consistent with the ownership terms expressed within this Security Agreement. The term "Subject Ideas or Inventions" includes any and all ideas, processes, trademarks, service marks, inventions, designs, technologies, computer hardware or software, original works of authorship, formulas, discoveries, patents, copyrights, copyrightable works products, marketing and business ideas, and all improvements, know-how, data, rights, and claims related to the foregoing that, whether or not patentable, which are conceived, developed or created which:

- Relate to ISC current or contemplated business, and/or plans, projects, or other matters which Authorized Agent operates, manages, controls, or for which Authorized Agent is responsible.
- Relate to ISC's actual or demonstrably anticipated research or development;
- Result from any work performed by the Authorized User for ISC;
- Involve the use of ISC equipment, supplies, facilities, trade secrets, or Confidential or Proprietary Information; or Result from the access to any of the ISC memoranda, notes, records, drawings, sketches, models, maps, customer lists, research results, data, formulae, specifications, inventions, processes, equipment, or other materials (collectively, "Materials").

To the extent permitted by the Illinois Employee Patent Act, 765 ILCS 1060/1 et seq., all right, title and interest in and to all Subject Ideas and Inventions, including but not limited to all registrable and patent rights which may subsist therein, and any information that constitutes all or part of a trade secret, shall be held and owned solely by ISC, and where applicable, all Subject Ideas and Inventions shall be considered works made for hire. Authorized Users will mark all Subject Ideas and Inventions with the ISC copyright or other proprietary notice as directed by ISC and shall take all actions deemed necessary by ISC to protect the rights therein.

7.0 Record of Distribution

OES is not designed to be distributed in the same manner as a hardcopy or electronic copy of a report or plan, as is the customary and traditional method of distribution. OES consists of multiple preparedness and planning modules, components, and discreet portions of plans and policies, with certain components being disseminated (distributed) to appropriate personnel or organizations dynamically when requested by an Authorized User, consistent with his/her Security Level. The Information in OES is disseminated primarily through a web-based application/Software as a Service. This distribution method has a significant advantage over traditional planning by combining a dynamic method of dissemination with advanced security measures, while also providing multiple levels of operational redundancy. OES is disseminated through the following methods:

- OES is accessed by the use of a web browser and may require an internet connection (hard-line or wireless), and is available to all Authorized Users, within their Security Level, as long as an internet connection to the server on which OES is hosted is available. OES is stored on two servers in separate locations to maintain the first level of operational redundancy.
- Select components of OES are stored on a limited number of laptops and external hard drives, updated monthly or as required, in a secure location at the direction of the OES Liaison to maintain the second level of operational redundancy.
- Certain sections of OES are printed periodically, quarterly or as required, to maintain the third level of operational redundancy.
- Outdated electronic copies of components of OES stored on Authorized Agent laptops are erased for security and version control purposes. Outdated printed documents are destroyed.

8.0 Disclaimers

8.1 Limitation of Liability

The Authorized Agent has reviewed, approved, and is ultimately responsible for the maintenance and relevancy of the Information contained within this electronic publication. ISC has taken every reasonably foreseeable step to assist Authorized Agent in making the Information as accurate as possible. ISC is not responsible for any errors or omissions or any loss arising from use of this system.

UNDER NO CIRCUMSTANCES, INCLUDING, BUT NOT LIMITED TO, NEGLIGENCE, SHALL ISC BE LIABLE FOR ANY SPECIAL OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OF OR THE INABILITY TO USE, OES EVEN IF ISC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION ON LIABILITY SHALL SURVIVE THE FAILURE OF ANY EXCLUSIVE REMEDY.

Applicable law may not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply everywhere. No advice or information, whether written or oral, obtained by the Authorized User from ISC shall create any warranty not expressly stated in this Security Policy. In no event shall ISC's total liability to anyone for all damages, losses, and causes of action, whether in contract, tort (including, but not limited to, negligence) or otherwise, exceed the amount paid by Authorized Agent as license fees in the twelve months preceding the date the such claim of liability is made.

8.2 Disclaimer of Warranties

OES IS LICENSED TO AUTHORIZED USERS "AS-IS." ISC MAKES NO WARRANTIES WITH RESPECT TO OES AS TO ITS USE OR PERFORMANCE OR THE RESULTS THAT MAY BE OBTAINED BY ITS USE. EXCEPT FOR ANY WARRANTY, CONDITION, REPRESENTATION OR TERM TO THE EXTENT TO WHICH THE SAME CANNOT OR MAY NOT BE EXCLUDED OR LIMITED BY LAW APPLICABLE TO THE AUTHORIZED USER IN HIS/HER JURISDICTION, ISC MAKES NO WARRANTIES OR REPRESENTATIONS (EXPRESS OR IMPLIED WHETHER BY STATUTE, COMMON LAW, CUSTOM, USAGE OR OTHERWISE) AS TO ANY MATTER, INCLUDING, WITHOUT LIMITATION, NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, INTEGRATION, DESIGN, SATISFACTORY QUALITY, SECURITY, OR FITNESS FOR ANY PARTICULAR PURPOSE.

WITHOUT LIMITING THE FOREGOING, ISC DISCLAIMS ANY AND ALL WARRANTIES THAT THE USE OF OES WILL BE ERROR-FREE, UNINTERRUPTED, TIMELY, SECURE, OR OPERATE IN COMBINATION WITH ANY PARTICULAR HARDWARE, SOFTWARE, SYSTEM OR DATA, OR THAT THE PROGRAM WILL MEET AUTHORIZED USERS' REQUIREMENTS OR EXPECTATIONS, OR THAT ANY STORED DATA WILL BE ACCESSIBLE, RETRIEVABLE, ACCURATE, RELIABLE, OR UNCORRUPTED, OR THAT THE PROGRAM OR THE SERVER(S) THAT MAKE OES AVAILABLE WILL BE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS.

8.3 Indemnification

The Authorized User agrees to indemnify and hold ISC and their subsidiaries, affiliates, officers, agents, and employees, harmless from any claim or demand, including reasonable attorney's fees, made by any third party due to or arising out of his/her use of OES, his/her violation of the terms and conditions of this Security Policy, or his/her violation of any rights of another person or entity.

9.0 Miscellaneous Provisions

9.1 Forum Selection and Choice of Law

This Security Policy shall be interpreted and construed according to, and governed by, the laws of the State of Illinois. The Circuit Court of Cook County shall have exclusive jurisdiction to hear any dispute under this Security Policy, and venue shall be proper there, or, if such court is without subject matter jurisdiction, the United States District Court for the Northern District of Illinois shall have exclusive jurisdiction and venue. The Authorized User consents to the exercise of personal jurisdiction over him by any Court, state or federal, situated within the Northern District of Illinois.

9.2 Changes to the Security Policy

ISC reserves the right to change any of the terms or conditions of this Security Policy at any time and from time to time. Such modified terms of this Security Policy shall become effective upon posting of a link to an updated version of this Security Policy on the log-in page through which OES may be accessed. Authorized Users agree that this posting of a link constitutes notice of any changes. Authorized Users agree to comply with the terms of this Security Policy, as it may be amended from time to time, and are responsible for regularly reviewing this Security Policy. Continued use of OES after any such amendments shall constitute consent to such changes.

9.3 Waiver

No waiver of any breach of this Security Policy shall be deemed a waiver of any preceding or succeeding breach of the same or any other provisions hereof. No such waiver shall be effective unless in writing signed by the party granting the waiver to the other party, and then only to the extent expressly set forth in that writing.

9.4 Severability

If any term of this Security Policy is found to be unenforceable or contrary to law, it shall be modified to the least extent necessary to make it enforceable, and the remaining portions of this Security Policy will remain in full force and effect.

9.5 Section Headings

The section headings appearing in this Security Policy have been inserted for the purpose of convenience and ready reference. They do not purport to, and shall not be deemed to, define, limit, or extend the scope or intent of the clauses to which they pertain.

9.6 Assignment

The limited license granted under this Security Policy is not assignable or transferable in any form or fashion, and Authorized Users agree not to attempt to assign, delegate, or transfer (whether by operation of law or otherwise) any rights or obligations under this Security Policy.

9.7 Survival of Certain Provisions

All provisions indicating an ongoing obligation shall survive any termination or expiration of this Security Policy or the limited license granted to an Authorized User hereunder but shall not imply

or create any continued right to use OES after the termination of this Security Policy or the limited license.

9.8 Entire Agreement

This Security Policy sets forth the entire understanding between an Authorized User and ISC with respect to the subject matter herein, and supersedes all prior written agreements, discussions and understandings, expressed or implied, between the parties concerning such matters. This Security Policy does not govern any other services or programs offered, owned or licensed by ISC, whether for free or for a payment, each of which will be governed by separate written contracts between the parties.

ISC OES CLIENT COOP SOG

Introduction

The Odysseus™ product suite marketed by Integrated Solutions Consulting (ISC) is a set of web-based tools targeted to support emergency management organizations with developing disaster management plans, managing exercises, tracking training and credentials, analyzing risks, and managing grants.

The heart of the product offering is the Knowledge Management System (KMS) module of the Odysseus™ product. This module offers preparedness professionals with a standard and consistent framework for defining disaster preparedness plans and sharing those plans across various levels of government. The product suite is offered as a hosted, software-as-a-service (SAAS) solution. New clients are configured within the framework and given authentication credentials.

Application Architecture

The product suite is developed and maintained by ISC's Technology Support Team (TST) using the Microsoft suite of web development technologies (.Net, Sql Server, IIS). Source Code is managed locally by the TST using the version control software, Subversion. The TST also manages the production environment and the Amazon hosting agreement.

The TST has a team of seven developers familiar with the system, three of which can manage the related server architecture. Most user content entered as HTML pages are stored in the SQL Server database. Attachments are stored in a file share area on the database server and stored in the database as links.

The TST recently implemented a report engine that allows users to generate a full PDF report of their content, processing the request as a background job. As part of the implementation, a scheduler framework was included but has not yet been exposed to end users.

Source code is managed using the version control software package Subversion. Source code includes application logic, configuration files, and scripts.

Software Development Profile

- Microsoft .Net Development IIS Middleware
- MS SQL Server
- MS Windows Server
- Storage of Images and Documents User Planning Content
- Version Control – Subversion
- SSL Logon Security Third Party Tools

Amazon Hosting Environment

The Odysseus™ product suite is provided as a hosted service to ISC clients. The production environment is hosted on dedicated servers with Amazon Web Services (AWS) on their EC2 plan.

The service level agreement commits to “99.95% monthly uptime”. The AWS plan allows ISC to scale its capacity on demand due to use of its virtual server configuration.

Access is managed within a specified IP range, with the ability to selectively expose IPs to the internet. Connections between the development environment at technology support team and the AWS production environment are managed with encrypted VPN connections.

Data Storage is bundled in the EC2 Plan as Elastic Block Store (EBS). This storage is configurable, mounted to specific instances, replicated in the AWS data center, and supports capturing snapshot images of the data. ISC has also purchased support for a backup database server and standby database/application server in a separate AWS data center location.

Default system monitoring is provided on a 5 minute frequency through AWS CloudWatch. The Management Console supports setting alerts for various performance thresholds, defining custom metrics, and capturing performance statistics. It is also used as an administrative tool to stop and start server instances, manage data volumes and configure security.

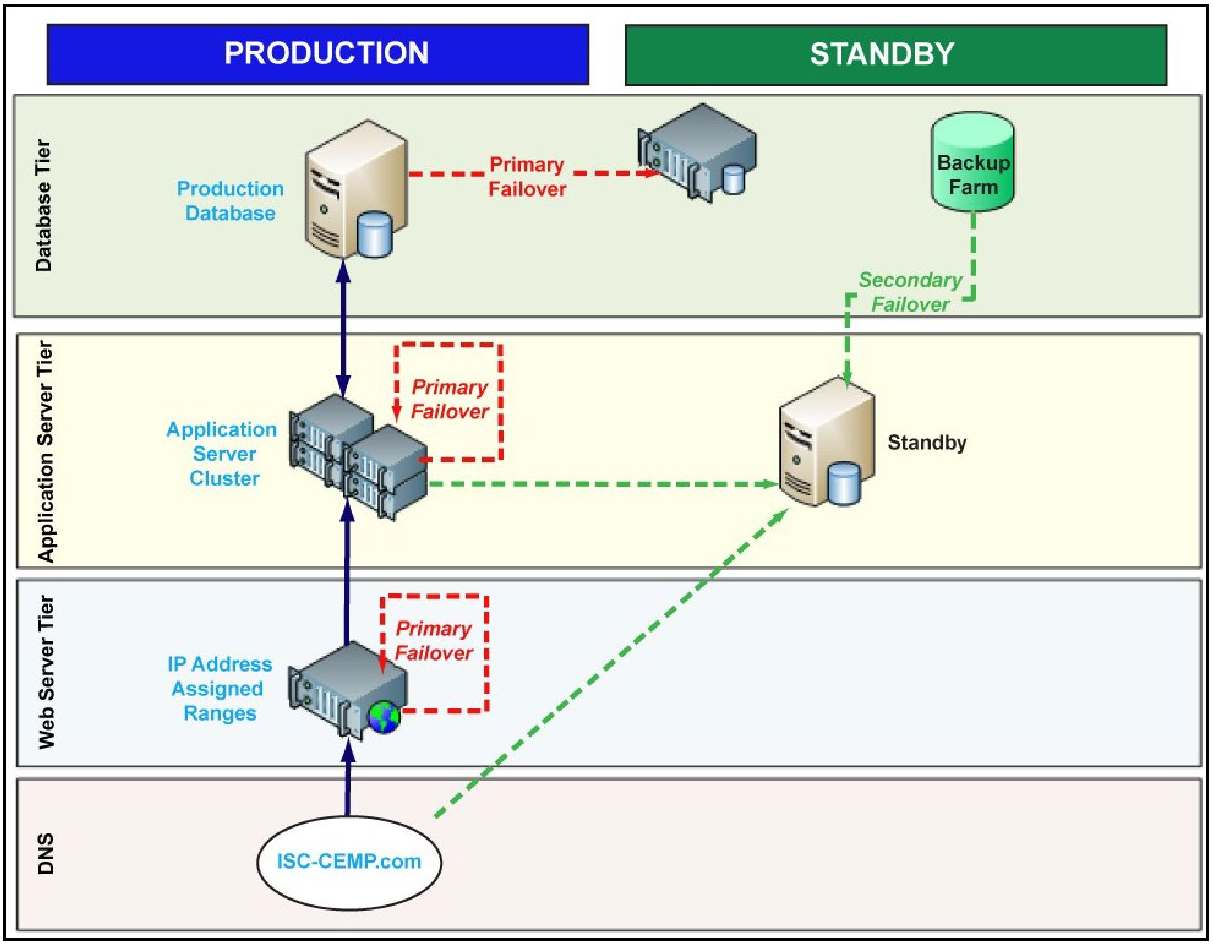
AWS will use commercially reasonable efforts to make Amazon EC2 and Amazon EBS each available with a Monthly Uptime Percentage (defined below) of at least 99.95%, in each case during any monthly billing cycle (the “Service Commitment”). In the event Amazon EC2 or Amazon EBS does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

“Monthly Uptime Percentage” is calculated by subtracting from 100% the percentage of minutes during the month in which Amazon EC2 or Amazon EBS, as applicable, was in the state of “Region Unavailable.”

“Unavailable” for Amazon EC2 means: when all of your running instances have no external connectivity.

Technology Infrastructure

A multi-tiered environment hosts production, standby, and development environments. Development is located on the TST premises, all other environments are hosted by Amazon Web Services. An overview of the AWS infrastructure is depicted in the diagram below.



Component details for each environment are provided in the table below.

	Production Environment	Standby Environment	Development
Location	Amazon EC2 Primary Data Center	Amazon Alternate Data Center	Technology Support Team (TST)
Database Servers	Primary	Standby - Configured as a full application, web, and database server ready for data load if necessary. URL can be redirected to this location.	TST DB Servers
Web Servers	Application Servers - Platform: IIS, WinServer		
Application Servers			
Load Balancing	Yes	None	N/A
Test Servers	N/A	Yes	TST DB Servers
Firewall and Web Tier	Yes		N/A
Backup Schedule	Nightly	None - Refreshed with each major production release	N/A

Source Code	Executables loaded to Application Servers	Executables loaded to Standby Server	Raw Source Code stored in TST version control system (SubVersion) plus 2 offsite backups
Hardware and Firmware Updates	Managed by Amazon	Managed by Amazon	Managed by TST
Platform Updates	Patches and Upgrades managed by TST		
Monitoring		N/A	N/A
SLA and Contract Terms	Amazon Web Services: 99.95% Regional Uptime. Any failures beyond SLA are resolved as credits to client account.		N/A

Database Structure

OES end users can define their plans directly online using built-in HTML editing. This data is stored in a SQL Server database that has several methods of recovery if necessary.

The system also supports the uploading of related resources such as documents, links, and images. These files are stored outside of SQL Server using a file share location on the database server. There is no built-in version management for these files, and restoration is limited to retrieving items manually from prior backups. Some clients use the document upload feature more heavily than the HTML editing method.

Current Usage

Average and peak usage statistics are useful in understanding the impact of an outage and the priority of mitigation strategies. Day-to-day usage is infrequent with the exception of a few organizations that are heavy users. System-wide user activity peaks annually during the period when related grant reporting is due.

Backup Management

System and Data backups are standard practice for application management both to support hardware and outage situations, and to support logical restoration of historical data. A comprehensive backup approach should ensure that both the database content and the application components are preserved and restorable.

Database Content	User Data stored in the SQL Server database is saved nightly. Nightly backups are archived for retrieval, currently without limit.
Data File and Media Content	Nightly backups are archived for retrieval.
Application Environment	Images of the Production Application servers are taken periodically and saved. The Standby Server is configured with a duplicate application environment with all executable components. In the event of a production environment outage, ISC Clients can be redirected to this server.
Source Code	Source code is stored on development servers using a version control system (Subversion) that tracks and preserves changes to the code base. Nightly copies of the version control library are sent to both an offsite local server, and cloud-based backup service.

System Monitoring

AWS CloudWatch provides system monitoring and a configurable Management Console tool. The Management Console supports setting alerts for various performance thresholds, defining custom metrics, and capturing performance statistics. The TST has configured the management console to produce alerts based on various triggers.

More typically the TST or a Customer will notice a problem first. In situations where a technical decision is needed to shift to a failover strategy, The TST will make the change and notify ISC.

Technical Safeguards

The Amazon Hosted Web Services (AWS) EC2 plan manages minor outages to servers automatically in a manner that would rarely be noticed by ISC or end users. The Production Database uses virtualized storage and can switch to a mirrored segment for localized server issues.

ISC and its TST have taken additional steps to address continuity should the AWS data center have an outage. Backup data and an imaged standby application server are located separately. Hardware failures are the most likely cause of system problems, and the most easily managed with best practices. These situations include:

- **Failure of a specific Web/App Server** – Traffic is immediately redirected to other Web/App Servers in the farm. ISC has 3 such servers and additional can be added virtually if traffic warrants it.
- **Database Disk Failure** – The Production Database uses virtualized storage and can switch to a mirrored segment for localized server issues. Failure would redirect to this image automatically. Potentially a specific transaction might need to be re-entered.
- **Database Crash / Corruption** – In a situation where the mirrored data is not sufficient, nightly backups to Amazon Glacier can restore data to the prior day's state. The restoration takes one hour.
- **Electrical Outage** – Data Centers are backed up with electrical generators. Short of a severe regional grid issue, these outages would not be noticed.
- **Data Center / Production Outage** – ISC has provisioned a standby server, in a separate AWS data center, that is fully configured with the application and database server environment. Upon partial or full failure of the production environment, this server can be loaded with the most recent database backup and serve as a temporary production environment. The standby environment is a cold standby, and would require an hour to be started and loaded with the latest data backup.
- **DNS Outage** – Though rare, this situation has been experienced by ISC. The domain hoster for the OES URL experienced an outage that prevented the URL's ability to navigate to the system location. In an extended outage, ISC could notify the users of a direct link into the production system at AWS.

Detection and Recovery Practices

Beyond technical infrastructure safeguards, successful disaster recovery relies on the policies, procedures, and people in place to manage the event. Procedures should encompass Detection, Communication, Failover Responsibilities, and Restoration Responsibilities. At a broad level, the following practices are in place.

	Production Data Center Failure	Client Site Technology/Access Failure	DNS Failure (URL Connection Down)
Scenario Description	A noticeable outage at AWS forces transition to Standby Env. Takes 3 hours to bring up last night's data. URL may or may not be redirected.	A client has lost their data center, including access to their ISC logon credentials. They need access to their plan.	The Website URL is down but the backend environment is functioning.
Detection Method	User Compliant System Monitor Alert AWS Notification	User contacts ISC	User compliant
Who is Notified?	ISC TST	ISC	Client may contact ISC
How is Support Contacted?	Normal communications to the TST use email, text, and cell phones. The TST also has a call center in Arizona that will keep escalating messages to team members until a response is received.	ISC may request information or a file restoration	ISC contacts the TST
How is ISC Contacted?	The TST contacts ISC	Client calls their normal support rep, if they have the phone number on them.	The TST or Client alerts ISC
Technical Failover and Restoration	The TST and AWS	N/A	The TST or Domain Host
Client Communications and Follow-Up	Per discretion of the support contract	N/A	N/A

Integrated Solutions Consulting (ISC) Support

Integrated Solutions Consulting (ISC) is dedicated to improving client preparedness and provides continual support to assist clients.

Communications

In the unlikely event of a system disruption, ISC will likely be aware of the situation, as staff are continually monitoring the system. However, clients should first contact their regional representative first to maintain chain of command prior to contacting ISC directly. In the event

that regional representatives are unavailable, clients should contact Odysseus Support for assistance by emailing support@odysseus-gmt.com.

Crisis Operations Checklist

ISC has Standard Operating Procedures and Guidelines to address outage and client emergency scenarios. Protocols address items such as:

- List of key contacts within the organization
- Responsibilities of staff members, with backups, so that there is no confusion as to who is doing what, or who is responsible for decisions
- Timeline expectations
- Communications approach methods for internal staff, TST, Clients, and external parties.
- List of related assets.

Unplanned Outage Scenario - An outage of the system or data center occurs. Duration is unknown.

	Activity	Description	Assigned To	Backup
☐	**a) Who is Notified First?**	System Outage alert from AWS, system monitor, user complaint	TST Contacts ISC Management	
☐	**b) Start Standby Setup**	Contact the TST to start the process of turning on Standby and loading the last database backup in case it is needed.	Manager 1	Manager 2
☐	**c) Contact Internal Staff**	Broadcast Email to All Staff Conduct Briefing Conference Call Schedule Followup Conference Call	Manager 1	Manager 2
☐	**d) Contact All Clients with Initial Information**	Broadcast Email to all Clients System Status Posting on Community Portal		
☐	**e) Contact Priority and Recent Clients**	Direct Calls to Priority Clients and clients that were logged on when the outage occurred (if known).	Client Rep	Rep Backup
☐	**f) Technical Monitoring Liaison with the TST**	Individual in contact with TST to determine extent and severity of problem.		
☐	**g) Wait or Cutover to Standby Decision**	Based on severity, determine whether to continue waiting for system restoration, or take action to invoke Standby.	Manager 1	Manager 2
☐	**h) Internal Staff Conference Call**	Internal Staff call to inform of major decisions and assign tasks.	Manager 1	Manager 2
☐	**i) Standby is Invoked**	Proceed with **Standby Environment Standup Procedures** (separate checklist/procedures)		
☐	**j) Restoration is Complete**	System is functional again. TST contacts ISC	TST to ISC	

☐	**k) Restoration Validation**	Internal procedure to validate logons and basic functionality		
☐	**l) Broadcast Restoration to Clients**	Broadcast Email to all Clients System Status Posting on Community Portal Special instructions if necessary.		
☐	**m) Contact Priority Clients**	Direct Calls to Priority Clients	Client Rep	Rep Backup
☐	**n) Review issues and lessons learned**	Review of the root cause of the issue and the effectiveness of the response with a goal of improving procedures and preventing of the same technical issue in the future.	ALL	