

## ACCESS AND USE POLICY

Authorized Users may access and use the Odysseus Enterprise System (OES) consistent with the terms contained within this Security Policy, and for the sole benefit of OES. Use of the 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 usernames 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 another person within YOUR ORGANIZATION, a Department, Trusted Partner, or Contractor must be individually registered and licensed to use the 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 the OES, or any portion thereof, without the express written permission of OES, 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 the OES by YOUR ORGANIZATION and/or ISC.

Each Authorized User agrees to notify YOUR ORGANIZATION and/or ISC of any known or suspected unauthorized use(s) of the 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.

YOUR ORGANIZATION will work collaboratively with ISC to optimally assign at its sole discretion the appropriate Security Level to each Authorized User. YOUR ORGANIZATION 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. Below are examples of security levels. Each OES Application has similar, customizable permission levels. Each Security Level encompasses those levels below it (e.g. Level Three access includes access to all information contained in Levels One and Two). The current Security Levels include, but are not necessarily limited to:

**Level One:** This Security Level will provide information for recently hired YOUR ORGANIZATION personnel, Departments, Trusted Partners, and Contractors. Level one Authorized Users have access to the horizontal navigation area (starting with Overview) and Situational Awareness Sections located in the index area.

**Level Two:** This Security Level will provide information for a more select group of YOUR ORGANIZATION personnel, Departments, Trusted Partners, and Contractors with greater rank, responsibilities, and/or a greater "need to know" the Information contained in Level Two. Level Two Authorized Users have access to the horizontal assistance area, Situational Awareness, and YOUR ORGANIZATION Operational Resources Sections located in the index area.

**Level Three:** This Security Level will provide information for selecting a more select group of YOUR ORGANIZATION personnel, Departments, Trusted Partners, and Contractors with greater rank, responsibilities, and/or a greater "need to know" the Information contained in Level Three. Level Three Authorized Users have access to the horizontal assistance area, Situational

Awareness, YOUR ORGANIZATION Operational Resources, and YOUR ORGANIZATION Operational Planning

**Level Four:** This Security Level will provide information for selecting a more select group of YOUR ORGANIZATION personnel, Departments, Trusted Partners, and Contractors with greater rank, responsibilities, and/or a greater “need to know” the Information contained in Level Four. Level Four Authorized Users have access to the horizontal assistance area, Situational Awareness, YOUR ORGANIZATION Operational Resources, YOUR ORGANIZATION Operational Planning, and Hazard Specific Planning Sections located in the index area.

**Level Five:** This Security Level will provide information for selecting a more select group of YOUR ORGANIZATION personnel, Departments, Trusted Partners, and Contractors with greater rank, responsibilities, and/or a greater “need to know” the Information contained in Level Five. Level Five Authorized Users have access to the horizontal assistance area, Situational Awareness, YOUR ORGANIZATION Operational Resources, YOUR ORGANIZATION Operational Planning, Hazard Specific Planning, and Preparedness and Planning Cycle Sections located in the index area.

**Administrator Level:** This Security Level is restricted to select YOUR ORGANIZATION management personnel. The Administrator Level Authorized Users to have access to the horizontal assistance area Situational Awareness, YOUR ORGANIZATION Operational Resources, YOUR ORGANIZATION Operational Planning, Hazard Specific Planning, and Preparedness, Planning Cycle, and Administrative Sections located in the index area.

**Super Administrator:** This Security Level is restricted to a more select YOUR ORGANIZATION management group. The Super Administrator Level Authorized Users have access to the horizontal assistance area, Situational Awareness, YOUR ORGANIZATION Operational Resources, YOUR ORGANIZATION Operational Planning, Hazard Specific Planning, and Preparedness, Planning Cycle, Administrative, and Super Administrative Sections located in the index area.