Applicability

This Crisis Response Policy ("Policy") applies to Insight Enterprises and all wholly owned subsidiaries of Insight worldwide (hereinafter collectively "Insight"). The Policy applies to all Insight teammates, contractors, and authorized representatives with equal effect.

Purpose

The specific purpose of this Policy is to establish a policy for the immediate reporting and handling of a crisis.

Definitions

- **Classification Level (Public)** - This classification applies to information that has been approved by Insight management for release to the public. Making the information public cannot harm the organization in any way.
- **"Crisis"** is defined as any global, regional, or local natural or human-caused event occurrence or business interruption:  
  (i) adversely impacting the Company’s operations, financial position, or reputation, or which runs the risk of escalating in intensity to the point at which it adversely impacts the Company’s operations, financial position, or reputation;
  (ii) causing harm to people or damage to property or the environment;
  (iii) falling under close media or government scrutiny or investigation, interfering with normal operations and wasting significant management time and or financial resources
  (iv) adversely affecting employee morale; or
  (v) jeopardizing the Company’s reputation, prospects, officers, or teammates, and, in any such instance, having a significantly negative impact on the Company.
- **“Crisis Response Team”** shall be comprised of the individuals listed on Exhibit A to this Policy, as such list may be amended from time to time.
• **GCO** – Global Compliance Office
• “**Responsible Officers or Individuals**” means the senior executive or executives in any location and the Country Manager, principal accounting or financial officer in the facility, and principal human resources officer in any Company facility.

**Policy Detail**

1. **Policy Introduction**
   1.1. Insight Enterprises, Inc. is a publicly traded global company subject to the laws of various jurisdictions and responsible to its shareholders, teammates and other stakeholders for the prompt and appropriate handling of a Crisis.

2. **Policy Statement**
   2.1. All teammates shall follow the below identified protocol if they become aware of an impending or actual Crisis.

3. **Crisis and Warning Signs**
   3.1. In most instances, there are warning signs that a crisis situation is developing or is about to happen. Identifying and reacting to these signs as soon as possible will enable Insight Enterprises, Inc. to mobilize the necessary resources. The warning signs of an impending crisis can include the following:

   3.1.1. An inquiry from a journalist or news organization that cannot be addressed using the prepared materials;

   3.1.2. An inquiry or statement from a government agency or media that alleges a problem with an Insight Enterprises, Inc. product, service or a company policy or practice;

   3.1.3. A data security situation that has the potential to attract external attention, delay product shipments or adversely affect clients, partners or vendors;

   3.1.4. Word that Insight Enterprises, Inc.’s competitors have been approached for comment by the media on company related issues;

   3.1.5. Any threat (or suggestion of a threat) against the company;

   3.1.6. Extreme weather conditions that threaten a local company facility;

   3.1.7. An unannounced visit by a member of the press or a regulatory or law enforcement agency; and

   3.1.8. Any communications - online or offline - from disgruntled clients, employees, shareholders, neighbours or third-party groups who may be motivated to cause problems for Insight Enterprises, Inc.

4. **Teammates Responsibilities**
   4.1. The primary interest of the Company in handling a Crisis is to protect the safety and well-being of the individual teammates or any other person(s) to whom Insight might owe a duty of care who may be affected by the Crisis (“Persons”).

   4.2. Accordingly, in the event of a Crisis, the Responsible Officer or Individuals shall
first report the matter to appropriate emergency services and/or local authorities if the Crisis requires immediate response to secure the safety and well-being of Persons and take such other actions as are necessary and prudent to protect the safety and well-being of Persons.

4.3. The Responsible Officer or Individual should follow the reporting obligations of Sections 4.4 and 4.5 (below) as early as practicable, but the safety and well-being of Persons should be the first priority.

4.4. In the event of a Crisis which does not threaten the safety or well-being of Persons or after any threats to the safety or well-being of Persons has subsided, the Responsible Officer or Individual shall next report the event to the Crisis Response Team. The Responsible Officer or Individual shall begin with the Crisis Response Team notification in numerical order (see Exhibit A). Once the Responsible Officer or Individual has obtained personal contact (not voicemail) with a Crisis Response Team member, the Responsible Officer or Individual shall not continue notification of the Crisis Response Team as the contacted Crisis Response Team member shall continue notifying the remaining Team members.

4.5. The Responsible Officer or Individual shall send a confirming email to the contacted Crisis Response Team member immediately following the phone call, stating very simply that a Crisis has occurred or is occurring, and briefly stating the nature of the Crisis. For purposes of the privacy laws of various countries, the confirming email should be brief and should contain only the essential facts required to alert the individuals on the Crisis Response Team of the existence of the Crisis and should not attempt to set out all the facts and circumstances.

4.6. Once the reporting procedures in Sections 4.4 and 4.5 of this Policy have been followed, the Crisis should be managed as directed by the Crisis Response Team. To the extent possible, the Crisis should not be discussed with any party outside the Company and should be managed as directed by the Crisis Response Team.

5. **Media Inquiries**

5.1. In the event of a media inquiry, do not engage in any discussions. Be polite with the media contact; however, indicate that you are not an authorized speaker for the organization. As soon as practical after the end of the inquiry, refer to Exhibit A and contact the Crisis Response Team for guidance. Sample responses for use during the media inquiry:

5.1.1. “I don’t know the answer to that question because that is not my area of expertise. However, I would be happy to look into it for you and get some to answer it for you.”

5.1.2. “Our executives may be better equipped to provide that information. Please let me know if you have any related questions and I’d be happy to find out who the right person is and call you back with a name and number or arrange a call.”

6. **Government Visits**

6.1. There may be occasions when a government entity visits an Insight location unannounced. A government official conducting an investigation should have a formal letter of authority, which may be a Warrant, a Subpoena (which does not give them the right to conduct a search), or a European Commission or other
6.2. Use the following as a checklist and make sure each step is followed (unless directed otherwise by the Crisis Response Team):

6.2.1. Upon arrival of the investigators, check the identity of the investigators and confirm the legal basis for their visit (i.e. read the Letter/Notice of Authority carefully and ensure the individual inspectors who have presented and identified themselves are authorised to conduct a dawn raid).

6.2.2. Obtain a copy of the Letter/Notice of Authority and/or warrant (if they have one).

6.2.3. Contact the most senior person on site (e.g., Responsible Officer) and any individual named in the letter. The Responsible Officer should take the lead in interaction with the government official.

6.2.4. Immediately contact the Crisis Response Team (see Exhibit A) in descending numerical order, once contact has been established (not voicemail), the contacted Crisis Response Team member shall continue notifying the remaining Team members.

6.2.5. Follow the usual visitor procedures and provide the usual site safety information.

6.2.6. Do not leave the investigators unattended.

6.2.7. Assign a “shadow” for each investigator and provide the shadow with a copy of the Letter/Notice of Authority and/or warrant.

6.2.8. Escort the investigators to a separate meeting room or rooms.

6.2.9. Make a separate meeting room available for Company personnel to use.

6.2.10. Office staff are to be instructed not to destroy documents or delete emails or discuss the investigation with anyone outside the office.

6.2.11. Ask the investigators to delay their investigation until you can receive instructions from the corporate Crisis Response Team. They will typically wait for up to one hour. Record any refusal to wait for instructions.

6.2.12. Ask the investigators to explain what the investigation is about and how they intend to proceed. Carefully record their response in writing.

6.2.13. Explain to the investigators that someone will be assigned to each investigator.


6.2.15. When the investigation is underway:

6.2.16. List the documents to be copied and keep records of all documents copied, set aside for review, or which are intended to be taken (see Exhibit B).

6.2.17. List the questions asked by the investigators (see Exhibit C).
7. **Policy Review**

7.1. The Policy owner will review the Policy regularly at least once every two years or as required.

8. **Reporting suspected violations**

8.1. Any suspected violation of an Insight policy or standard should be reported without delay to the GCO at compliance@insight.com or Insight Compliance Helpline http://insightenterprises.ethicspoint.com

8.2. Insight has a strict no retaliation policy and will not tolerate any kind of retaliation against anyone who, in good faith, reports a violation of Insight policy or law. If you have questions or problems concerning this Policy, you should contact the GCO (compliance@insight.com).

**Related Policies, Procedures and Guidance**

- NIST-IS002

**Version History**

<table>
<thead>
<tr>
<th>Version Date</th>
<th>Version Number</th>
<th>Version Changes</th>
<th>Authorized By</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/1/2021</td>
<td>1.0</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>10/4/2021</td>
<td>2.0</td>
<td>Added ‘7. Annual Review” and made formatting changes.</td>
<td>Lisanne Steinheiser, Global Compliance Officer and Assistant Secretary.</td>
</tr>
</tbody>
</table>
| 08/22/2022   | 3.0            | • Updated Crisis Response Team members  
• CLASSIFICATION LEVEL: Public | Lisanne Steinheiser, Global Compliance Officer and Assistant Secretary. |
## EXHIBIT A

### Crisis Response Team Call Tree

#### Event Response Team – Contact Information

<table>
<thead>
<tr>
<th>Na</th>
<th>E-mail</th>
<th>Direct</th>
<th>Cell</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Glynis Bryan, CFO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sam Cowley, SVP &amp; General Counsel</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Joyce Mullen, CEO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Summa Nallapati, CIO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amy Protexter, SVP, Marketing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dee Burger, President, NA Region</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emma De Sousa, President, EMEA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EXHIBIT B
Document Record

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recorded by (sign):  
______________________________________________________________________

Print Name:  
______________________________________________________________________

Date: ________________

Page _____ of _____
# EXHIBIT C

## Questions Log

<table>
<thead>
<tr>
<th>Question</th>
<th>Document related to Ref. Num.</th>
<th>Response</th>
<th>Interviewee</th>
<th>Lawyers consulted prior to response Y/N</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Recorded by (sign):
______________________________

Print Name:
______________________________

Date: ____________________________

Page _____ of _____