Security Incident Response Plan

1. The person who discovered the incident contacts the support service via e-mail **support@sprutcam.com** or through the contact information indicated on the website **www.sprutcam.com**
   Persons who discovered the incident may be dealers, application users, or **SprutCAM Tech** employees.
   Sources that may request contact information may include:
   - Support service;
   - Personnel monitoring intrusion detection;
   - System Administrator;
   - Business partner;
   - Manager;
   - Security department or security officer.

These persons can request contact information from those who discovered the incident, including information about license numbers, contact numbers, e-mail and details of the incident.
Each of these sources has contacts for communication with IT department specialists responsible for resolving the incident.

2. If the person who discovered the incident is from the IT department or the affected department, they will proceed to **step 5**.

3. If the person who discovered the incident is not an employee of the IT department or the affected department, he will send an e-mail to **support@sprutcam.com** and duplicate the message via internal chats to general groups of the IT department.

4. Security will consult the IT emergency contact list or affected department contact list and inform employees in the order listed. The security service will register:
   a. Caller's name;
   b. Call time;
   c. Contact information about the caller;
   d. the nature of the incident;
   e. What equipment or people were involved?
   f. Location of equipment or persons involved;
   g. How the incident was discovered;
   h. When the event was first noticed, which confirmed the assumption that the incident occurred.

5. The IT department employee or affected department employee who receives the message (or discovers the incident) will consult their contact list to contact both management and incident response personnel. The employee will inform those on the list. The employee will contact the Incident Response Manager using email and telephone messages, while ensuring that other appropriate and reserve personnel, as well as assigned managers, contact him. The employee will register the information received in the same format as the security service did in the previous step. The employee might add the following:
   a. Is the affected software business critical?
   b. What is the severity of the potential impact?
   c. The name of the target system, as well as the operating system, IP address and location;
   d. IP address and any information about the source of the attack.

6. Contacted response team members will meet or discuss the situation via group chat and determine a response strategy.
    a. Is the incident real or alleged?
    b. Is the incident still ongoing?
    c. What data or property is at risk and how critical is it?
    d. What will be the business consequences if the attack is successful? Minimal, severe or critical?
    e. What system or systems are being attacked, where are they located physically and online?
    f. Is the incident located within a trusted network?
    g. Is the response urgent?
    h. Can the incident be quickly contained?
    i. Will the response alert the attacker and do we care?
    j. What kind of incident is this? Example: virus, worm, invasion, abuse, damage.

7. An incident record will be created. The incident will be classified at the highest applicable level of one of the following categories:
    a. The first category is a threat to public safety or life;
    b. The second category is a threat to confidential data;
    c. Category three – Threat to computer systems;
    d. Category four – Interruptions in the provision of services.

8. Team members will develop and follow one of the following procedures based on their response to the incident assessment:
    a. Worm response procedure;
    b. Virus response procedure;
    c. System failure procedure;
    d. Procedure for active response to intrusion. Is important data at risk?
    e. Procedure for responding to an inactive intrusion;
    f. System Abuse Procedure;
    g. Procedure for responding to property theft;
    h. Procedure for responding to a denial of service on a website;
    i. Procedure for responding to a denial of service of a database or file;
    j. Procedure for responding to spyware.

The team may create additional procedures not provided for in this document. If there is no applicable procedure, the team should document what was done and then establish a procedure for the incident.

9. Team members will use forensic techniques, including reviewing system logs, searching for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the victim of the incident to determine how the incident was caused. Only authorized personnel should conduct interviews or examine evidence, and the composition of authorized personnel may vary depending on the situation and organization.

10. Team members will recommend changes to prevent the incident from recurring or infecting other systems.

11. After management approval, changes will be implemented.

12. Team members will provide instructions to restore the system to an uninfected state. They can do any or more of the following:
    a. Reinstalling the affected system from scratch and, if necessary, restoring data from

backup copies. Before doing this, you must preserve the evidence;
   b. Force users to change passwords if passwords could be intercepted;
   c. Ensure that the system is protected by disabling or removing unused services;
   d. Make sure that the system is completely updated;
   e. Ensure that real-time virus protection and intrusion detection are working;
   f. Ensure that the system records the correct events and at the appropriate level.

13. Documentation – the following are documented:
   a. How the incident was discovered;
   b. Category of incident;
   c. How the incident occurred: via email, firewall, etc;
   d. Where the attack originated from, such as IP addresses and other relevant information about the attacker;
   e. What was the response plan;
   f. What was done in response?
   g. Was the reaction effective?

14. Preservation of evidence - copies of logs, emails and other communications are made. Lists of witnesses are kept. Evidence is retained for as long as necessary to complete prosecution and in the event of an appeal.

15. Notify relevant external authorities - notify the police and other relevant authorities if prosecution of the perpetrator is possible. List agencies and contact numbers here.

16. Assess Damage and Cost - Assess the damage to the organization and estimate both the cost of the damage and the cost of containment efforts.

17. Review response policies and updates - plan and implement preventive measures to ensure the intrusion does not reoccur.
   a. Consider whether additional policies could have prevented the invasion;
   b. Consider whether a procedure or policy was not followed that allowed the intrusion, and then consider what can be changed to ensure compliance with the procedure or policy in the future;
   c. Was the response to the incident adequate? How can it be improved?
   d. Was each relevant party informed in a timely manner?
   e. Were the incident response procedures detailed and covered the entire situation? How can they be improved?
   f. Have changes been made to prevent re-infection? Have all systems been patched, systems locked, passwords changed, antivirus updated, email policies configured, etc.?
   g. Have changes been made to prevent new or similar infections?
   h. Should any security policies be updated?
   i. What lessons were learned from this experience?