# TCWGlobal's Security Incident Response Plan

## Contents


Purpose and Scope ..... 2
How to Recognize a Security Incident ..... 3
Roles and Responsibilities ..... 3
Responsibilities ..... 4
External Contacts ..... 5
Incident Response Plan Steps ..... 6
Appendix A ..... 9
Non Compliance with TCWGlobal's Security Policy ..... 10
Testing and Updates ..... 10


| | |
|---|---|
| Policy Area | Security Operations Team |
| Approved Date | 8/28/2023 |
| Approved By | Erica Ostberg, Tom Kucharski, Jaime Nguyen, Zack Abdou |
| Effective Date | 8/28/2023 |
| Current Version | V3.5 |

| Policy History | | | |
|---|---|---|---|
| Version | Date | Description | Approved by |
| V.3.6 | 8.28.2023 | Updated Contacts | Erica Ostberg, Tom Kucharski, Jaime Nguyen, Zack Abdou, Leslie Cruz |
| V 3.5 | 2/2/2023 | Updated contacts | Erica Ostberg, Tom Kucharski, Jill Arldt, Jaime Nguyen, Zack Abdou, Leslie Cruz |

| | | | |
|---|---|---|---|
| V 3.4 | 10/11/22 | Updated contacts | Erica Ostberg, Tom Kucharski, Jill Arldt, Jaime Nguyen |
| V 3.3 | 6/13/2022 | Updated internal and external contacts to reflect changes in staff and external support. | Erica Ostberg, Tom Kucharski, Rachel Altman, Casey Beebe, Jill Arldt |
| V 3.2 | 2/4/2022 | Updated with proper internal SIRT team members and with current Cyber Insurance Policy | Erica Ostberg, Andy Waggoner, Zack Abdou, Justin Black, Casey Beebe |
| V3.1 | 10/1/2021 | Updated with new company name and logo, and law firm first contact per risk management/Breach coach discussion with Scott Koller | Robyn Ise, Erica Ostberg, Andy Waggoner, Marisa Farwell, Justin Black |
| V3 | 1/6/2021 | Complete overhaul and rewrite in new format | Robyn Ise, Erica Ostberg, Andy Waggoner, Marisa Farwell, Justin Black |
| V2.1 | 2/7/2020 | Updates per Robyn | Robyn Ise, Samer Khouli, Andy Waggoner |
| V2 | 2/15/2018 | Updates per Robyn | Robyn Ise, Samer Khouli, Andy Waggoner |
| V1.0 | 6/28/2017 | Version 1.0 | Samer Khouli, Andy Waggoner |

## Purpose and Scope

All security incidents must be managed in an efficient and time effective manner to make sure that the impact of an incident is contained and the consequences for our business and customers are limited. This document sets out TCWGlobal's plan for reporting and dealing with security incidents.

# TCWGlobal's Security Incident Response Plan

**What is a Security Incident?**

A Security Incident means any incident that occurs by accident, or deliberately, that impacts any of our business systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services in TCWGlobal, including our client's data.

## How to Recognize a Security Incident

A security incident may not be recognized immediately; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within our environment. Some examples are below.

Note that in most cases we have tools in place to watch for, alert, and remediate these issues automatically, however, if YOU see something that looks suspicious, please notify a team member or our CTO immediately:

- Excessive or unusual login and system activity, especially from any inactive user accounts
- Watch out for excessive or unusual remote access activity. This could be relating to staff or third party providers
- The occurrence of any new wireless (Wi-Fi) networks visible or accessible from your environment
- The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executables and programs. This could be on our network, your computer, in email, etc.
- Hardware or software keyloggers found connected to or installed on systems
- Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain any company data

## Roles and Responsibilities

TCWGlobal's security incident response plan must be followed by all personnel. This includes all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of TCWGlobal, working with TCWGlobal's or our customers' data or on TCWGlobal premises. For simplicity, all of these personnel are referred to as 'staff' within this plan.

### *Roles*

The TCWGlobal **Security Incident Response Team (SIRT)** is comprised of:

| Role* | SIRT Responsibility | Name | Email | Telephone |
|---|---|---|---|---|
| **CTO/CISO** | **Incident Response Lead** | Tom Kucharski | Tom.kucharski@tcwglobal.com | 858-705-8962 |

| | | | | |
|---|---|---|---|---|
| **Director of IT** | Incident Response Technical Lead | Zack Abdou | zack.abdou@tcwglobal.com | 916-220-4103 |
| **SecOps/Lead Programmer** | *StaffingNation* Incident Response Technical Lead | Tom Kucharski | Tom.kucharski@tcwglobal.com | 858-705-8962 |
| **CCO** | Compliance Lead<br><br>Legal questions/issues/ communications relating to security incidents | Erica Ostberg | Erica.ostberg@tcwglobal.com | Office: 858-810-3323<br><br>Cell:619-922-6647 |
| **Human Resources, Mgr** | Handling of any personnel and disciplinary issues relating to security incidents | Jaime Nguyen | Jaime.Nguyen@tcwglobal.com | 858-810-3020 |
| **COO** | Operation Lead<br><br>Handling of customer communications and response | Leslie Cruz | Leslie.cruz@tcwglobal.com | 858-810-3119 |

## Responsibilities

The **Incident Response Lead** is responsible for:

- Ensuring that the Security Incident Response Plan and associated response and escalation procedures are defined and documented, to ensure the handling of security incidents is timely and effective.
- Review, test, and update the plan yearly.
- Ensure the Security Incident Response Team are properly trained, at least once each year.
- Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan, as and when needed.
- Reporting to and communicating with external parties, including clients, legal representation, law enforcement, etc. as is required.
- Authorizing onsite investigations by appropriate law enforcement as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.

**Security Incident Response Team (SIRT)** members are responsible for:

- Making sure that all staff understand how to identify and report a suspected or actual security incident.
- Advising the Incident Response Lead of an incident when they receive a security incident report from staff.

- Investigating each reported incident.
- Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident.
- Gathering, reviewing and analyzing logs and related information from various central and local safeguards, security measures and controls.
- Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
- Reporting each security incident and findings to the appropriate parties. This may include third party service providers, business partners, customers, etc., as required.
- Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions.
- Resolving each incident to the satisfaction of all parties involved, including external parties.
- Initiating follow-up actions to reduce likelihood of recurrence, as appropriate.
- Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All TCWGlobal staff members are responsible for:

- Making sure they understand how to identify and report a suspected or actual security incident.
- Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT)
- Reporting any security related issues or concerns to management, or to a member of the SIRT
- Complying with the security policies and procedures of TCWGlobal. This includes any updated or temporary measures introduced in response to a security incident (e.g. for business continuity, incident recovery or to prevent recurrence of an incident).

## External Contacts

| External Party | Contact Name | Email | Telephone |
|---|---|---|---|
| **Law firm Baker Hostettler** | Call the 855 number for 24/7 hotline to lawyer team/breach coaches | | 855-217-5204 24/7 hotline |
| **Cyber insurance Policy - Houston Casualty Policy and Excess Cyber Policy Details** | Call 1-888-627-8995 to file a claim<br><br>Primary Cyber Coverage – Tokio Marine HCC Policy#H21NGP209993 | support@eplaceinc.com | Breach Coach: 1-877-244-9688 |

| | | | |
|---|---|---|---|
| | Excess Coverage – Sunstone Assurance Policy#JJ-1-DIC 2020 | | |
| **Chosen Forensics firms (2)** | Kivu Consulting \| www.kivuconsulting.com (investigation + ransomware)<br><br>Kroll Cyber Security \| www.kroll.com<br><br>Charles rivers – phishing incident | | |
| **Vinebrook (SOC responsibilities for StaffingNation)** | | tcw@vinebrookmsp.com | |
| **Artic Wolf (Cybersecurity team for TCW Global)** | | security@articwolf.com | |
| **San Diego Computer and Technology Crime High Tech Response Team :CATCH" Team** | | https://catchteam.org/ | (619) 531-3150 |
| **FBI San Diego Field Office** | Suzanne Turner is the special agent in charge for SD | https://www.fbi.gov/contact-us/field-offices/sandiego | (858) 320-1800 |

## Incident Response Plan Steps

There are a number of steps and stages that must be taken to make sure that we protect our business by reacting to a security incident appropriately.

### *Report*

1. Information security incidents must be reported, ASAP, to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT). The member of the SIRT receiving the report will advise the Incident Response Lead of the incident.

In the event that a security incident or data breach is suspected to have occurred, we recommend the staff member discuss their concerns with their manager, who in turn may raise the issue with a member of the SIRT.

## *Investigate*

1. After being notified of a security incident, the SIRT will perform an initial investigation and determine the appropriate response, which may be to initiate the Security Incident Response Plan.

   If the Security Incident Response Plan is initiated, the SIRT will investigate the incident and initiate actions to limit the exposure of data in mitigating the risks associated with the incident.

## *Containment*

1. Isolate compromised systems from network and unplug any network cables – without turning the systems off.
2. If applicable, change the SSID on the WAP and other systems that may be using this wireless network (but not on any of the systems believed to be compromised).
3. Preserve all logs and similar electronic evidence, i.e. logs from firewall, anti-virus tool, access control system, web server, application server, databases, etc.
4. Perform a back-up of your systems to preserve current state – this will also facilitate any subsequent investigations.
5. Keep a record of ALL actions you and all members of the SIRT take.
6. Stay alert for further indications of compromise or suspicious activity in the environment.
7. If possible, gather details of all compromised or potentially compromised accounts.

## *Inform*

Once the SIRT has carried out their initial investigation of the security incident:

1. The Incident Response Lead will alert the SIRT's senior management primary contact.
2. The Incident Response Lead and / or the SIRT personnel responsible for communications will inform all relevant parties. This may include a call to Hiscox, local law enforcement, and other parties that may be affected by the compromise such as our customers, business partners and suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation.

## *Maintain Business Continuity*

1. The SIRT will engage with our operational teams to make sure that our business can continue to operate while the security incident is being investigated.

## *Resolve*

1. The SIRT will work with external parties, including law enforcement, etc., to ensure appropriate incident investigation (which may include onsite forensic investigation) and gathering of evidence, as is required.
2. The members of the SIRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational.
3. The Incident Response Lead will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders (including your acquirer, local law enforcement, etc.) as is needed.

## *Recover*

1. The Incident Response Lead will authorize a return to normal operations once satisfactory resolution is confirmed.
2. The SIRT will notify the rest of the business that normal business operations can resume. Normal operations must adopt any updated processes, technologies or security measures identified and implemented during incident resolution, and all updates or changes must be documented and training performed.

## *Review*

The SIRT will complete a post-incident review after every security incident. The review will consider how the incident occurred, what the root causes were and how well the incident was handled. This will help to identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

- Updates to the Security Incident Response Plan and associated procedures.
- Updates to our security or operational policies and procedures.
- Updates to technologies, security measures or controls
- The introduction of additional safeguards in the environment where the incident occurred (for example, more effective malware protection).
- The SIRT Executive Officer/Risk Owner (the senior management primary contact) will ensure that the required updates

and changes are adopted or implemented as necessary.

# Appendix A

## *Specific Incident Response Types*

Some specific incident types requiring additional response actions are provided below.

***Malware (or Malicious Code)***

1. Disconnect devices identified with malware from the network IMMEDIATELY. Remember to look for a wired as well as wireless connection.
2. Disable the user's account immediately (if applicable)
3. Examine the malware to identify the type (e.g. rootkit, ransomware, etc.) and establish how it infected the device, in order to understand how to remove it.
4. Once the malware has been removed a full system scan must be performed, to verify it has been removed from the device.
5. If the malware cannot be removed from the device, it must be tagged as breached, and the user issued a new device.
6. A full scan of all network devices may be necessary
7. Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.
8. The user's credentials must be changed
9. The breached device must be fully wiped, and rebuilt.

***Unauthorized Wireless Access Points***

If unauthorized wireless access points are detected, or reported by staff, these must be recorded as a security incident.

1. SIRT will investigate to identify the location of the unauthorized wireless access point/device.
2. The SIRT will investigate as to whether or not the unauthorized wireless access point/device is being used for a legitimate business purpose/need. If a legitimate business reason is identified, then this wireless access point or device must be reviewed and go through the correct management approval process. This is to make sure that the business justification is documented and the wireless access point/device is securely configured (e.g. change default passwords and settings, enable strong authentication and encryption, etc.).
3. All other unauthorized wireless access points/devices must be located, shutdown and removed.

***Loss of Equipment***

1. The theft or loss of an asset, such as a PC, laptop or mobile device, must be reported immediately to a member of the SIRT and local law enforcement. This includes losses/thefts outside of business hours and on weekends.

2. If the device that is lost or stolen contained sensitive or customer data and the device is not encrypted, SIRT will complete an analysis of the sensitivity, type and volume of data stolen. With this said, all devices at TCWGlobal have disk-based encryption configured.
3. In the case of a mobile device registered in our MDM policy, SIRT will initiate a remote wipe. Evidence should be captured to confirm this was successfully completed.

## Non Compliance with TCWGlobal's Security Policy

Any deliberate or accidental actions that are in breach of TCWGlobal's security policy, including systems or data misuse, unauthorized exposure of data to external parties, or unauthorized changes to systems or data.

1. SIRT will engage with the relevant business area to establish an audit trail of events and actions. They will determine who is involved in the policy violation and the extent of the violation.
2. SIRT and/or manager will notify Human Resources of the incident.
3. SIRT will work with Human Resources and manager to determine whether disciplinary action is needed.
4. SIRT will undertake an assessment of the impact and provide advice and guidance to the business area to prevent reoccurrence, for example, retraining of staff.

## Testing and Updates

Annual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the SIRT are aware of their obligations, unless real incidents occur which test the full functionality of the process.

1. The Incident Response Plan will be tested at least once annually, per our Incident Response Policy.
2. The Incident Response Plan Testing will test our business response to potential incident scenarios to identify process gaps and improvement areas.
3. The SIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to SIRT members.