Data Breach Incident Response Policies

Changes, Revisions, and Reviews

Date	Name	Revision(s)
09-NOV-2021	J. Goepel	Updated to reflect changes in management and corporate policies.
12-NOV-2020	J. Goepel	Document updated to reflect changes in vendor teams.
05-OCT-2020	J. Goepel	Document updated to reflect changes to WISP.
01-APR-2020	J. Goepel	Document created to memorialize ad hoc and unwritten policies already existing within COMPANY.

Incident Response Team:

Internal Team:

Lead: Emilia Rodriguez – Mobile: 856-555-3472

Alternate Lead: Nick Alexson – Mobile: 267-555-5473

Coordinator: Alex Nicholson – Mobile: 215-555-5577

Internal PR/Media: Sloane Christiansen - Mobile: 571-555-5547

External Team:

Outside Breach Counsel: Harris Smith – 222-222-2222

Forensics and Incident Response Vendor: Brown Incident – Artie Brown - 877-777-8888

Information Technology ("IT") Vendor: Perpetual Uptime – Jerome Bennett – 215-555-4433

Managed Security Services ("MSS") Vendor: Absolutely Perfect Cybersecurity - 267-555-3783

External PR/Media – WeGotYou Inc. – Wanda Reynolds – 222-333-5577

Cyber Strategy Vendor: Lowe Price Consulting – Richard Lowe – 703-555-9997

Policies:

1) Overview:

Mavis's Machine Shops ("COMPANY") recognizes that cybersecurity and data privacy are important considerations in today's digital world. COMPANY also understands that Customer data will likely be the subject of a breach even as we continue our investments and efforts to keep it safe. COMPANY is committed to responding quickly and decisively to any suspected or confirmed cybersecurity or data privacy incident, especially those involving Customer data (collectively an "Incident"). COMPANY has crafted this Data Breach Incident Response Plan (this "Plan") to help those responding to an inevitable Incident.

2) Reporting and Responding to a Suspected or Confirmed Incident

Any suspected or confirmed Incident must immediately be reported to the **Coordinator**, and all Firm employees must provide their immediate and full cooperation to the **Coordinator's** efforts related to the Incident. The **Coordinator** must ensure the procedures set forth herein are promptly followed by the identified person(s) or vendor(s).

3) Communicating Outside COMPANY about a Suspected or Confirmed Incident

Suspected or confirmed Incidents involve a number of legal and regulatory issues and must be handled appropriately. Therefore, the only persons and/or vendors, including COMPANY employees, who are authorized to speak with the media or others outside COMPANY about any suspected or confirmed Incident are the **External PR/Media** contact and the **Lead**. The **Lead** is expected to allow the **External PR/Media** contact to facilitate any necessary messaging. Notwithstanding the foregoing, if the **External PR/Media** contact is absent or unavailable and where the media is actively seeking comment from COMPANY, the **Internal PR/Media** contact may respond to the media's inquiry after consultation with the **Lead**. At no time are the **Coordinator**, **Forensics and Incident Response Vendor**, **IT Vendor,** or any Firm employees authorized to speak with anyone outside COMPANY, including without limitation speaking with members of the media or posting on social media or other online forums, about any suspected or confirmed Incident. Notwithstanding the foregoing, the **Coordinator**, **Forensics and Incident Response Vendor**, **IT Vendor,** and any Firm employees may speak about the Incident with individuals outside COMPANY (e.g., the **Coordinator**, **Forensics and Incident Response Vendor**, or **IT Vendor**)who are actively involved in the Incident response.

4) Engaging External Team:

The **Coordinator** will work with the **Outside Counsel** to engage the **External Team** identified above prior to a breach so the members of the **Incident Response Team** are familiar with one another and are better prepared to respond to an Incident.

5) Procedures Testing:

i. Internal Testing - The **Internal Team** will meet at least semi-annually to test the Plan using tabletop exercises created by COMPANY or COMPANY**'s Cyber Strategy Vendor**. These tabletop exercises will help ensure that the **Internal Team** members are familiar with the Plan and techniques for operationalizing it.

ii. Internal and External Testing - The **Internal Team** and **External Team** will meet to test the Plan at least once a year (ideally at one of the **Internal Team** meetings) using a combination of tabletop and nondestructive real-world testing. The testing will help ensure that the **Team** members are familiar with the Plan and techniques for operationalizing it.

iii. Plan Updates - The **Coordinator** will oversee updates to the Plan based on lessons learned during the testing.

6) Internal Team Responsibilities

i. The Lead - The **Lead** identified above is responsible for making, or delegating the making of, any necessary decisions, including without limitation setting/reviewing approaches to messaging, and for authorizing deviations from this Plan.

ii. The Alternate Lead - The **Alternate Lead** identified above is only involved in this Plan in the event the **Lead** is unavailable or incapacitated, in which case the **Alternate Lead** is authorized to act as the **Lead**.

iii. The Coordinator - The **Coordinator** identified above is responsible for managing the efforts of the different parties involved in responding to an Incident, and for adjudicating any disputes or reconciling any differences of opinion between **External Team** members. The **Coordinator** must ensure that all members of the **Internal Team** have each other's contact information, and the contact information for all members of the **External Team**, stored on at least one of their respective mobile devices and in hard copy form outside COMPANY's offices. The **Coordinator** must routinely, and no less than annually, review the contacts identified above and the procedures described herein to ensure they are consistent with COMPANY's then-current business processes, personnel, and vendors. The **Coordinator** shall log all such reviews in the Changes, Revisions, and Reviews log at the beginning of this Plan. In the event the **Coordinator** is unavailable or incapacitated during an Incident response, the **Lead** will also act as **Coordinator**.

7) External Team Responsibilities

i. The **Internal PR/Media** contact identified above is responsible for coordinating the messaging of COMPANY's efforts with media, regulators, and law enforcement.

ii. The **Outside Counsel** identified above is responsible for engaging and overseeing the work of other outside consultants, including the **Forensics and Incident Response Vendor,** the **IT Vendor**, and the **PR/Media** team, as part of any incident response.

iii. The **Forensics and Incident Response Vendor** is responsible for conducting a forensic analysis of the Incident, including evidence preservation and remediation of the underlying Incident cause(s). With the approval of the **Coordinator**, the **Forensics and Incident Response Vendor** may direct the **IT Vendor** to undertake certain actions and may act in the place of the **IT vendor** as the situation dictates.

iv. The **IT Vendor** is responsible for managing the operation of COMPANY's computer and telecommunications equipment, including, without limitation:

1. ensuring systems are properly backed up, and can be restored from backup, consistent with COMPANY's Written Information Security Plan;
2. testing the backup equipment;
3. ensuring COMPANY's antivirus and other security-related tools are up to date, including any corresponding malware signatures or other indicators of compromise, consistent with COMPANY's Written Information Security Plan;
4. applying patches and other software updates to COMPANY's computer and telecommunications equipment in a timely manner consistent with COMPANY's Written Information Security Plan;
5. maintaining the operation of uninfected/unaffected equipment; and,
6. otherwise ensuring that COMPANY can continue operations during an Incident to the greatest extent possible while not unnecessarily impeding the work of the **Forensics and Incident Response Vendor** or others involved in the Incident response.

v. The **Managed Security Services** vendor is responsible for the security of COMPANY's computing systems, including, without limitation:

1. ensuring patches and other software updates have been properly applied to all equipment in accordance with COMPANY's Written Information Security Plan;
2. scanning COMPANY's computer and telecommunication equipment for known vulnerabilities, reporting any found vulnerabilities to the **Coordinator**, and working with the **IT Vendor** to remediate any vulnerabilities found in a timely manner;
3. ensuring appropriate logging is enabled on all computer and telecommunications equipment and monitoring log files and other alerts for any anomalous activity or indicators of compromise;
4. responding to any alerts or other anomalous activity in accordance with this Incident Response Plan; and,
5. working with COMPANY to enhance COMPANY's cybersecurity program to respond to new and different threats in accordance with COMPANY's risk management approach.

Data Breach and Incident Response Plan:

1) Preparation

a. Make Copies of the Plan Available

i. Although a master copy of this Plan will be stored in electronic form with COMPANY's other policies and procedures, the **Coordinator** will also maintain a sufficient quantity of paper copies at COMPANY's offices such that the entire Team can have copies in the event COMPANY's systems are, or must be taken, offline. All Team members will also store electronic copies of the Plan outside COMPANY's systems for their reference.

2) Detection and Analysis

a. Determine Whether an Incident has Occurred

i. Collect Background Information - Record contact information for the person reporting the Incident (the "**Incident Reporter**"), the contact information for the **Coordinator,** the date and time the Incident was first reported, and, where available, the date and time the Incident was first discovered, on a copy of the Customer Data Breach Response Worksheet (the "Worksheet") that is attached as Appendix A. Record the details provided by the **Incident Reporter** in the Incident Details section of the Worksheet. Mark the Incident as Under Investigation by placing a check mark next to Investigating under the Incident Details section of the Worksheet.

ii. Basic Actions Based on Incident Type – The appropriate next steps will vary based on the type of Incident that has been reported.

1. Stolen Physical Property Containing Customer Data - If the Incident involves the theft of physical property (e.g., the theft of a laptop, server, portable media, physical files, etc.) as reported by a Firm employee, contact local law enforcement immediately and record the contact information for the primary and alternate law enforcement officer(s) on the Worksheet. Record the date and time at which the Incident was first discovered and reported in the Incident Details section of the Worksheet. Record the address from which the physical property was stolen in the Incident Started field of the Incident Details section of the Worksheet, and the addresses from which the incident was first discovered and first reported in the corresponding fields in the Incident Details section of the worksheet. These facts are sufficient to determine that an Incident has occurred, and you should proceed to 2)b., below.
2. IT Vendor, MSS Vendor, and Firm Employee Reports - If the **Incident Reporter** is the **IT Vendor** and/or the **MSS Vendor**, record the **IT Vendor** and/or **MSS Vendor** contact information in the Other Team Members Involved section of the Worksheet. Work with the **Incident Reporter** to fill in as many details as are available in the Incident Details section of the Worksheet. An Incident report by the IT Vendor, the MSS Vendor, or a Firm employee is sufficient to determine that an Incident has occurred and you should proceed to 2)b., below.
3. Internally Maintained Software - If the **Incident Reporter** is an internally maintained tool and that tool identifies a potential data breach, you should:
    a. Make two copies of any log files associated with the tool and any recent reports generated by the tool.
    b. Store one of the log file copies in a safe place, preferably off-site.

c. Record as many details as are available in the Incident Details section of the Worksheet and continue to 2)b, below.

4. Reports from Law Enforcement or Regulators – If the **Incident Reporter** is or purports to be a law enforcement officer or regulatory official:
   a. Record the physical location involved in the report in the appropriate field in the Incident Details section of the Worksheet, if relevant and available.
   b. Record the contact information for the **Incident Reporter** in both the Incident Reporter and Primary Law Enforcement Officer/Regulator fields on the Worksheet.
   c. Record the **Incident Reporter's** supervisor's information in the Worksheet;
   d. Independently verify the supervisor's contact information (e.g., by calling a publicly-available telephone number for the organization employing the **Incident Reporter** and supervisor and validating that they are employees and their contact information).
   e. Initiate contact with the supervisor to ensure that the report is legitimate.
   f. If the supervisor confirms the details in the report, record this information in the Response Actions Performed section of the Worksheet. The supervisor's confirmation of the details is sufficient to determine that an Incident has occurred and you should proceed to 2)b.
   g. If the supervisor does not confirm the details, record the time and date of the conversation and the fact that the supervisor was unable to corroborate the report in the Response Actions Performed section of the Worksheet. You should consult with the **Lead** to determine whether to stop the response at this point, or to further engage actual law enforcement or regulatory personnel.
5. Reports from Independent Security Researchers – If the **Incident Reporter** is or purports to be an independent security researcher (e.g., a "white hat hacker" or "ethical hacker"), their report may include a request for compensation and a timeline for response before the Incident is publicly disclosed. This is a standard industry practice in the ethical hacker community and should not be viewed by COMPANY as an overtly aggressive act. The **Incident Reporter** chose to disclose the Incident to COMPANY in a constructive manner (i.e., without notifying the media or authorities) that allows COMPANY to decide how best to proceed. The **Incident Reporter's** disclosure of the Incident in this manner will likely save COMPANY significant costs over alternative disclosure methods that could have been used.
   a. Record the nature of the report (i.e., that it was disclosed by an ethical hacker) in the Incident Description portion of the Incident Details section of the Worksheet along with all details provided by the **Incident Reporter**.
   b. Using information from the report, fill in as many details as are available in the Incident Details section of the Worksheet, but do NOT contact the **Incident Reporter** for additional details.
   c. COMPANY will endeavor to reply to the **Incident Reporter** within one (1) business day with: a) a confirmation of receipt; and b) an assurance that the report is being processed through internal channels and that COMPANY will provide an additional reply within one (1) business week. The foregoing response should be sent by the **External PR/Media** contact, except where the **External PR/Media** contact is unable to respond within the reply timeline specified in the previous

sentence in which case the **Internal PR/Media** contact must reply within the aforementioned timeline.

d. Log the contact information for the person responsible for replying to the **Incident Reporter** in the Other Team Members section of the Worksheet. Record the actions taken in the Response Actions Performed section of the Worksheet, including the date(s) and time(s) that the Team Members were notified of the need for a reply, the person replying, the content of each reply, and the content of each reply.

e. Proceed to 2)b., below, after initiating the reply process and logging the appropriate information in the Worksheet.

6. Other Reports – If the **Incident Reporter** is any other third party, additional, independent corroborating information will be needed before an Incident should be declared. You should fill in as many details as possible in the Incident Details section of the Worksheet and proceed to 2)b.

b. Collect Relevant Impact Factors

i. Mark Incident Status - Place a check mark next to the Ongoing Attack and Investigating status indicators under the Incident Details section of the Worksheet.

ii. Identify the Affected Resources - List the resources (networks, subnets, hosts, etc.) in the Affected Resources section of the Worksheet. Supply the IP address(es), functionality (e.g., E-mail server, external accountant, end-user workstation, copier, etc.), and equipment name(s) for each affected resource.

iii. List Known Attack Vectors and Indicators of Compromise – Collect information regarding how the incident occurred or was identified, and any indicators of compromise.

iv. Information Involved – Identify the nature of the information that may have been involved in the Incident. This includes, without limitation, the type of information (e.g., healthcare records, banking/financial information, personally identifiable information, case histories, E-mail and written correspondence, etc.) and the jurisdictions of the data subjects (i.e., those individuals about whom the information pertained).

c. Quantify Incident Impact

i. Use the Impact Quantification Factors worksheet to assign a Severity Score to the Incident.

d. Declare Incident and Report to Appropriate Personnel

i. Examine the Severity Score of the Incident.

1. If the Incident is determined to be a Critical or High incident, contact the **Lead** and alert the Lead of the severity. The Lead shall contact **Outside Breach Counsel** immediately and will contact the **Coordinator**. Skip ahead to 2)d.ii.

2. If the Incident is determined to be a Moderate or Low severity, contact the **Coordinator** immediately and advise the Coordinator of the Incident and the Severity Score. The **Coordinator** should determine, with input from the **Lead**, whether to involve **Outside Breach Counsel** at this time.

ii. Identify Relevant Jurisdictions and Determine Breach Notification Window. Many jurisdictions require that an organization experiencing a data breach notify the State Attorney General or other individuals within a specific time period. It is important to ensure that the Incident response meets these legal and regulatory requirements.

3) Containment, Eradication, and Recovery

a. Contain the Incident

Containing the incident is an important part of an incident response. In some cases, it may be prudent to disconnect the equipment from the network or shut down the equipment to help contain the incident. However, such actions may cause the loss of important evidence that could help identify the perpetrator, while delaying such actions may result in significantly more data loss. The **Lead** is authorized to make the final decision as to whether to prioritize shutting down the equipment over preserving data. In general, if the Severity Score is Critical, the **Lead** should prioritize shutting down the equipment to prevent additional loss. If the Severity Score is High or Moderate, or if the Incident is continuing to spread, the **Lead** should prioritize disconnecting the impacted equipment from the network. If the Severity Score is Low, the Lead should prioritize preserving evidence. Document the steps taken to contain the Incident in the Response Actions Performed section of the worksheet below.

b. Acquire, Preserve, Secure, and Document Evidence

Ensure that, where possible, log files and memory dumps from relevant equipment are preserved and copied to removable media. That removable media must be carefully labeled so that others are aware that it: a) contains critical information, and b) may be infected by whatever is causing the Incident. All efforts taken to maintain the evidence should be documented in the Response Actions Performed section of the worksheet below.

c. Eradicate the Incident

i. Identify and mitigate all vulnerabilities that were exploited. This may involve the removal of equipment, updating of hardware/software, or other actions.
ii. Remove malware, inappropriate materials, and other components added by the attackers during the Incident.
iii. If more affected equipment is detected, repeat detection and analysis procedures to identify any other potentially affected equipment before repeating the containment and eradication processes.

d. Recover from the Incident

i. Implement additional monitoring, as needed, to look for future related activity.
ii. Return Affected Systems to Operationally Ready State. Returning to the Operationally Ready state too soon could result in reinfection or additional issues. The **Lead** is solely authorized to determine when equipment is ready to return to the Operationally Ready state.
iii. Confirm that affected systems are functioning normally. Record all findings in the Response Actions Performed section of the worksheet below.

4) Post-incident Activity

a. Gather Additional Evidence

Record any additional information, including any comments and notes from those involved in responding to the Incident, in the Post Incident Analysis section of the worksheet. This includes identifying those attributes of this Incident Response Plan that went well and those that need adjustment.

b. Create Follow-up Report

A follow-up report should be created which documents actions that have and will be taken to reduce the likelihood of similar events occurring in the future.

c. Hold Lessons-learned Meeting and Update Incident Response Plan

A meeting should be held with all Team members to discuss what went well and what could use improvement. That information should be consolidated and used to update this Incident Response Plan.

Appendix A –Data Breach and Incident Response Worksheet

1) Contact Information for primary Law Enforcement Officer/Regulator (if appropriate):

Name: _____

Role: _____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: _____

E-mail Address: _____

Phone Number: _____

2) Contact Information for alternate Law Enforcement Officer/Regulator (if appropriate):

Name: _____

Role: _____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: _____

E-mail Address: _____

Phone Number: _____

3) Contact Information for the Incident Reporter:

Name: _____

Role: _____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: _____

E-mail Address: _____

Phone Number: _____

4) Contact Information for COMPANY Incident Response Coordinator:

Name: _____

Role: _____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: _____

E-mail Address: _____

Phone Number: _____

5) Contact Information for COMPANY Incident Response Lead:

Name: _____

Role: _____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: _____

E-mail Address: _____

Phone Number: _____

6) Other Team Members Involved:

Name: ____

Role: ____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: ______________

E-mail Address: ______________________________________

Phone Number: ______________________________________

Name: ____

Role: ____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: ______________

E-mail Address: ______________________________________

Phone Number: ______________________________________

Name: ____

Role: ____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: ______________

E-mail Address: ______________________________________

Phone Number: ______________________________________

Name: ____

Role: ____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: ______________

E-mail Address: ______________________________________

Phone Number: ______________________________________

Name: ____

Role: ____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: ______________

E-mail Address: ______________________________________

Phone Number: ______________________________________

Name: ____

Role: ____

Organizational Unit (e.g., agency, department, division, team) and Affiliation: ______________

E-mail Address: ______________________________________

Phone Number: ______________________________________

7) Incident Details:

Current status of the Incident (updated as appropriate, choose all that apply):

___ Ongoing Attack | ___ Contained | ___ Eradicated | ___ Recovery | ___ Post-Incident Analysis

___ Investigating | ___ Impact Evaluated | ___ Formal Incident Declared | ___ Incident Closed

Status change date/timestamps (including time zone) when:

Incident Started: _____

Incident First Discovered: _____

Incident Reported: _____

Incident Declared: _____

Incident Resolved/Ended: _____

Physical location at which the:

Incident Started: _____

Incident First Discovered: _____

Incident Reported: _____

Source/cause of the incident (if known):

IP/Physical Address(es)	Individual/Equipment Name(s)	Notes

Incident Description (how was the incident detected, what occurred, etc.):

(Continue the description on one or more separate pages as necessary)

Affected Resources (e.g., networks, subnets, hosts, applications, data), including hostnames, IP addresses, and function:

(Continue the affected resources list on one or more separate pages as necessary)

Vectors of Attack and Indicators of Compromise (e.g., equipment not showing up in inventory, traffic patterns, registry keys, MD5/SHA256 hashes, etc.):

(Continue the attack vectors and IOC list on one or more separate pages as necessary)

Information Attributes (e.g., what kind of information (including healthcare information, banking information, PII, Customer information, and partner information) and from what jurisdiction(s)):

(Continue the Information Attributes on one or more separate pages as necessary)

8) <u>Impact Quantification Factors</u> (functional impact, information impact, recoverability, etc.):

Factor Description	Individual Factor Severity Score					Total
<u>Business Impact</u>	None (0)	Few/ Limited (2)	Many/ Moderate (5)	Most/ Severe (8)	All/ Critical (10)	
To what extent will the Incident or the response to the Incident impact COMPANY's ability to continue day-to-day operations?						
To what extent will the Incident impact one or more Customers' ability to continue day-to-day operations?						
To what extent is the Incident spreading to other equipment/information?						
<u>Information</u>	None (0)	Few/ Limited (5)	Many/ Moderate (8)	Most/ Severe (10)	All/ Critical (15)	**Total**
How many Customer-related health records may have been exposed in the Incident?						
How many Customer-related financial records may have been exposed in the Incident?						
How many Customer-related records containing Personally Identifiable Information (PII) may have been exposed in the Incident?						
How many firm employee financial or personal records, including PII, may have been exposed in the Incident?						
To what extent is/are COMPANY's bank account(s) impacted by the Incident?						
To what extent is COMPANY's confidential information impacted by the Incident?						
How much of the information impacted by the Incident is likely to be subject to additional legal or regulatory restrictions (e.g., GDPR, CCPA, 23 NYCRR 500, etc.)?						
<u>Recoverability Effort</u>	None (0)	Few/ Limited (5)	Many/ Moderate (8)	Most/ Severe (10)	All/ Critical (15)	**Total**
What is the expected level of effort needed to recover from the Incident?						
<u>Potentially Mitigating Factors</u>	None (0)	Few/ Limited (-5)	Many/ Moderate (-8)	Most/ Severe (-10)	All/ Critical (-15)	**Total**

To what extent is the information impacted by the Incident encrypted where the encryption key was not also exposed?						
Other Severity Factors	None	Few/ Limited	Many/ Moderate	Severe/ Most	All/ Critical	**Total**
Total Score						

Assign an overall Severity Score to the Incident based on the Total Score from the table above:

Low	Moderate	High	Critical
0-10	11-25	26-50	51+

9) Response Actions Performed (e.g., disconnected device from the network, shut down host/device, etc.):

(Continue the response actions description on one or more separate pages as necessary)

a. Log of Actions Taken by Incident Responders:

Date	Time	Incident Responder	Action Taken

(Copy sheet or add notes on back/separate page(s) as necessary)

10) Post Incident Analysis:

a. List of Evidence Gathered:

b. Incident Handler/Involved Party Comments and Notes:

c. Incident Cause (e.g., unpatched equipment, misconfigured application, zero-day, SQL injection, etc.):

d. Incident Business Impact:

11) Lessons Learned

a. What went well?

Document the actions taken or other attributes of the response that went well. This is important because any issues/improvements that may be listed below can be modeled after the successful attributes of the response.

b. What could use improvement?

What attributes of COMPANY's response could use additional attention?

c. How can we improve the Incident Response Plan for next time?