# Magento Incidence Response plan

## Section 1 - Incidence Response Team

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Role** | **Name** | **Email** | **Phone** | **Backup** | **Notes** |
| **Incident Leader** |  |  |  |  |  |
| **Management/Stakeholder** |  |  |  |  |  |
| **IT/Engineering Contact** |  |  |  |  |  |
| **Communications** |  |  |  |  |  |
| **Legal Representative** |  |  |  |  |  |
| **External Resource #1** |  |  |  |  |  |
| **External Resource #2** |  |  |  |  |  |
| **External Resource #3** |  |  |  |  |  |

## Section 2 – Rejection / Acceptance Criteria

## A close up of a sign Description automatically generated

|  |  |
| --- | --- |
| * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

### How will you keep a record of actions taken during the incidence response?

A close up of a logo

Description automatically generated

* What data points will be kept?
* How will it be stored?
* Where it be stored?
* What level of granularity should be taken?
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Section 3 – Breach & Severity Classification

A picture containing text

Description automatically generated

Create a list of types of breaches your site is susceptible to:

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Edit the following table to determine where acceptable severity levels lie for your merchant

|  |  |  |
| --- | --- | --- |
| Breach Rating | Merchant Liability | Customer Data Affected |
| 0 - Minor | No significant impact on any individual/group of individuals. Media interest very unlikely. | **MINOR** Breach of confidentiality. Only a single data subject affected. |
| 1 - Low | Damage to an individual’s reputation or possible misuse of their personal data. Media interest possible. | Breach is potentially serious but <10 data subjects affected and/or risk assessed as **LOW** e.g. files were encrypted. |
| 2 – High | Damage to a Merchant’s reputation. Media interest possible but it may not penetrate the public domain. | Potential serious breach & risk assessed as **HIGH** e.g. unencrypted special category records lost. Breach impacts on <50 data subjects. |
| 3 - Serious | Damage to the merchant’s reputation. Possible key local media coverage. | **SERIOUS** breach of confidentiality e.g. up to 100 data subjects affected e.g. loss of personal data relating to redundancies where data subjects clearly identifiable. |
| 4 - Severe | Damage to merchant’s reputation. Breach impacts on >20 but < 50 data subjects. Local media coverage of the breach. | **SEVERE** breach with either sensitivity/special category personal data e.g. credit card records or up to 1000 data subjects affected. |
| 5 - Critical | Damage to Merchant’s reputation. Breach impacts on >50 data subjects. National media coverage. | **CRITICAL** breach with the potential for identity theft and/or over 1000 data subjects affected. |
| 6 - Penalties | Breach will carry a monetary penalty. | **PENALTIES** apply. Restitution to affected data subjects. Other liabilities such as legal costs will be substantial. |

### Define what classified and sensitive data needs to be protected

A close up of a logo

Description automatically generated

* Database
* Magento Logs
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Create a list of specific steps each team member will need to take to investigate a category of breach and define, what data will be retrieved and who is responsible for getting it.

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### What are the criteria for making a decision to disrupt operations of the Magento store during investigation?

* Loss of Admin access
* Active breach stealing > 500 cards per hour
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Section 4 – Immediate Action Activities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity** | **Incident Lead** | **IT Contact** | **Legal Representative** | **Communications Coord** | **Management** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Section 5 – Approximate Timeline Activities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity** | **Incident Lead** | **IT Contact** | **Legal Representative** | **Communications Coord** | **Management** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## 

## Section 6 – Identify Attack Vector Activities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity** | **Incident Lead** | **IT Contact** | **Legal Representative** | **Communications Coord** | **Management** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Section 7 – Precise Timeline Activities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity** | **Incident Lead** | **IT Contact** | **Legal Representative** | **Communications Coord** | **Management** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Section 8 – Remove Persistent Threat Activities

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Activity** | **Incident Lead** | **IT Contact** | **Legal Representative** | **Communications Coord** | **Management** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

## Section 9 –Communication Requirements

### What are your external communication requirements?

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### What are your internal communication standards for keeping everyone in the IRT in sync?

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### What are your reporting requirements?

A picture containing object

Description automatically generated

* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_