# Example Escalation Matrix

## Step 1: Evaluate the Impact

The following table can be used when evaluating the level of crisis management and escalation required.

| **Impact type** | **Severity** |
| --- | --- |
| **Negligible** | **Low** | **Medium** | **High** |
| Risk to individualsafety – for eitheryour staff orfollowers | No risk to thepersonal safetyof anyindividual. | Some personalsafety risk in low chancecircumstances. | Risk of nonseriousharm tothe affectedindividuals. | Risk of seriousharm to theaffectedindividuals. |
| Risk ofmisinformation orbullying fromaudience – suchas inundation offalse information,excessivenumbers offake/sarcasticcommentary orsystematicharassment. | No risk ofmisinformationor bullying fromaudience. | Some risk ofmisinformationor bullying fromaudience in low chancecircumstances. | Serious risk ofmisinformation orbullying fromaudience in low chancecircumstances. | Serious risk ofmisinformation orbullying fromaudience in high chancecircumstances. |
| Organisationalembarrassmentor damage toreputation – suchas legal, HR,privacy issues ornon‐compliancewith relevantrequirements. | No risk ofembarrassmentor reputationaldamage. | Minorembarrassmentor reputationaldamage in low chancecircumstancesthat are unlikelyto be released. | Short‐termembarrassmentor reputationaldamage that doesnot have longterm effects forNSWGovernment. | Seriousembarrassment orreputationaldamage that mayhave long termeffects for theorganisation. |
| Breach ofinformation orpolicy – such asphishing attacksor scams, breachof data or humanerror. | Easily identifiedand quicklyfixed at thesource. | Easily identifiedsource that canbe fixed withsome additionalknowledge. | Source requiresassistance of IT oranother expertsto identify andfix. | Source is difficultto identity and/orfix even with theassistance ofexperts. |
| Threat to theorganisation’sability tocontinue toperform its socialfunctions – suchas a communitymanager or theentire social teamlosing access totheir social page. | No threat to theorganisation’sability tocontinue toperform itsfunctions. | Some threat tothe ability of oneor a fewindividualswithin theorganisation toperform some oftheir duties for ashort time. | Threat to theability of someindividuals’ abilityto perform dutiesfor an extendedperiod of time, ora threat to theability of somebusiness unity toperform someduties for a shorttime | Significant threatto the ability ofsome individualsor business unityto perform someor all of the dutiesfor an extendedperiod of time, orthreat to theability of one ofmore businessunits to performtheir functionentirely |

## Step 2: Consider the response

The following flow chart can be used to determine what should occur depending on the impact type identified in the above table.

**Step 3: Evaluate the responses**

After the crisis has been resolved, collate the data surrounding the issue and evaluate whether this was the best course of action.

## Step 4: Preventing future crises

As a part of the evaluation, consider mitigation strategies for this issue in future scenarios. Similarly, to what has occurred with the data breach policy, you should:

1. Evaluate areas that were unaccounted for
2. Evaluate whether the addition of future support would assist this issue in future situations.