## Example Escalation Matrix

**Step 1: Evaluate the Impact**

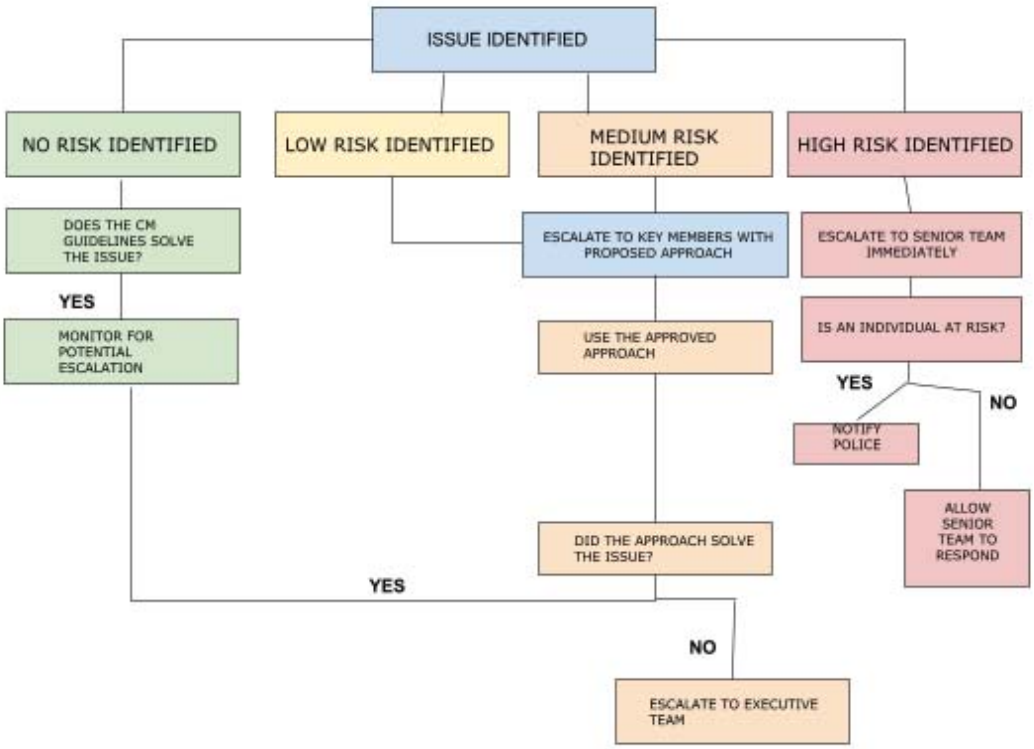
The following table can be used when evaluating the level of crisis management and escalation required.

| Impact type | Severity<br>Lowest | | | Highest |
|---|---|---|---|---|
| | Negligible | Low | Medium | High |
| Risk to individual safety – for either your staff or followers. | No risk to the personal safety of any individual. | Some personal safety risk in low-chance circumstances. | Risk of non-serious harm to the affected individuals. | Risk of serious harm to the affected individuals. |
| Risk of misinformation or bullying from audience – such as inundation of false information, excessive numbers of fake/sarcastic commentary or systematic harassment. | No risk of misinformation or bullying from audience. | Some risk of misinformation or bullying from audience in low-chance circumstances. | Serious risk of misinformation or bullying from audience in low-chance circumstances. | Serious risk of misinformation or bullying from audience in high-chance circumstances. |
| Organisational embarrassment or damage to reputation – such as legal, HR, privacy issues or non-compliance with relevant requirements. | No risk of embarrassment or reputational damage. | Minor embarrassment or reputational damage in low-chance circumstances that are unlikely to be released. | Short-term embarrassment or reputational damage that does not have long term effects for NSW Government. | Serious embarrassment or reputational damage that may have long term effects for the organisation. |
| Breach of information or policy – such as phishing attacks or scams, breach of data or human error. | Easily identified and quickly fixed at the source. | Easily identified source that can be fixed with some additional knowledge. | Source requires assistance of IT or another experts to identify and fix. | Source is difficult to identity and/or fix even with the assistance of experts. |

| | | | | |
|---|---|---|---|---|
| Threat to the organisation's ability to continue to perform its social functions – such as a community manager or the entire social team losing access to their social page. | No threat to the organisation's ability to continue to perform its functions. | Some threat to the ability of one or a few individuals within the organisation to perform some of their duties for a short time. | Threat to the ability of some individuals' ability to perform duties for an extended period of time, or a threat to the ability of some business unity to perform some duties for a short time | Significant threat to the ability of some individuals or business unity to perform some or all of the duties for an extended period of time, or threat to the ability of one of more business units to perform their function entirely |

**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 response**
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. Similar to what has occurred with the data breach policy, one should:

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