INCIDENT SEVERITY AND INFORMATION SHARING COLOR CODES

Incident Severity

Incidents are categorized based on the severity of potential or actual impact to the university. The graphic below shows the color code as used in the Weekly IT Security Report provided to the UW-Madison CIO and University Leadership. Color codes are supported by a short narrative statement that summarizes the major impact of the incident.

Risk Rating Color Code

Color Code for Risk Rating	Event in progress with significant loss of primary capability	**Critical**
	Realized impact to the university	**High**
	Potential significant impact to the university	**Medium**
	No significant events	**Low**

Example Report

Emerging Threat Intelligence	The Cybesecurity team became aware of large distributed denial of service attack on the Dyn managed domain name system (DNS) infrastructure that caused outages to several major websites including Box, Twitter and Reddit. No impact noted at UW-Madison. More information can be found at: https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/	Low

Information Sharing

Information sharing strategy follows the Department of Homeland Security Traffic Light Protocol (based on the draft *Guide to Cyber Threat Information Sharing* (NIST Special Publication 800-150) used by the US Computer Emergency Response Team as displayed in the graphic below.

When should it be used?	Color	How may it be shared?
Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	RED	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	AMBER	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	GREEN	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	WHITE	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Infographic Provided by the Office of Cybersecurity - https://it.wisc.edu/about/office-of-the-cio/cybersecurity/