THE DEPARTMENT OF
TECHNOLOGY & INNOVATION
we support you

ONE ALBUQUERQUE
cabq.gov/dti

cybersecurity traffic light readiness
CATEGORY DEFINITIONS

GREEN (LOW-RISK)

Systems and networks are operating normally with no known significant threats. Security measures are effectively preventing breaches, and all systems are up to date with patches and security updates.

EXAMPLES

1. Normal probing of the network
2. Low-risk viruses

YELLOW (ELEVATED-RISK)

Potential threats or vulnerabilities have been identified, but there is no immediate risk to systems or data. Additional monitoring and precautionary measures are in place while the situation is being evaluated.

EXAMPLES

1. An exploit for a critical vulnerability exists that has the potential for significant damage
2. A critical vulnerability is being exploited and there has been a moderate impact

ORANGE (HIGH-RISK)

A specific and credible threat has been identified, or a vulnerability has been exploited, but the impact is not yet severe. Immediate action is required to contain and mitigate the threat before it escalates.

EXAMPLES

1. An exploit for a critical vulnerability exists that has the potential for severe damage
2. A critical vulnerability is being exploited and there has been significant impact

RED (CRITICAL-RISK)

An active threat or breach has been detected with severe impact, or a critical vulnerability poses an immediate and significant risk to systems or data. Immediate and comprehensive response is necessary to contain and resolve the situation.

EXAMPLES

1. Complete network failures
2. Mission-critical application failures
3. Compromise or loss of administrative controls of critical systems