

When to Report Cyber/Data Information Security Incidents to the Department of Administration

- The term "breach" has legal significance and the definition varies based upon a multitude of applicable state and federal laws. A potential cyber/data information security issue should be referred to as an "incident" and not a "breach" until a final determination has been made by the Department of Administration and the State's commercial insurance carriers.
- For purposes of reporting potential incidents to the Department of Administration, breach means the unauthorized acquisition of data/information that:
 - (a) materially compromises the security, confidentiality, or integrity of the personal information maintained by a state agency or by a third party on behalf of the state agency.
 - (b) uniquely identifies an individual and may be of a sensitive nature.

"Personal Information"

- Per Montana Code 2-6-1501, "Personal Information" means
 - (a) First name or first initial and last name in combination with any one or more of the following data elements when the name and the data elements are not encrypted:
 - (i) Social security number;
 - (ii) Driver's license number, state identification card number, or tribal identification or enrollment number;
 - (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a person's financial account;
 - (iv) Medical record information as defined in 33-19-104 MCA;
 - (v) A taxpayer identification number; or
 - (vi) An identity protection personal identification number issued by the United States internal revenue service.
 - (b) "Personal Information" does not include publicly available information from federal, state, local, or tribal government records.

How to Report Cyber/Data Information Security Incidents to the Department of Administration

- Upon discovery or notification of a potential Cyber Attack, Cyber Incident, Data Information Incident, the state agency or university that maintains the information shall notify the Risk Management & Tort Defense Division and the state's Chief Information Officer immediately.
- The immediate supervisor must assure that the "Report of Incident" form <http://rmt.d.mt.gov/claims/agenciesreportclaims> is accurately completed, signed, and sent to the Risk Management & Tort Defense Division within 2 business days.
- If the incident has the potential of a release of personal information, do not contact individuals.
- Do not contact law enforcement agencies. After the Risk Management & Tort Defense Division has been notified of the incident, we will notify legal counsel and determine what to report to law enforcement agencies and when.
- Risk Management & Tort Defense Division insurance carrier for Cyber/Data incidents has specific requirements. Contact the Risk Management & Tort Defense Division immediately at 406-444-2421 if you have any questions regarding coverage. Cyber Risk Management Tools are available at <https://www.beazley.com/en-US/cyber-customer-centre/cyber-risk-management-tools/>.