

**Town of Crestone  
Resolution #**

**007 -2017**

**A RESOLUTION ADOPTING A DATA SECURITY  
POLICY FOR THE TOWN OF CRESTONE**

**WHEREAS**, the Town of Crestone is a member in the Colorado Intergovernmental Risk Sharing Agency (CIRSA) who provides general liability insurance; and

**WHEREAS**, CIRSA has recommended that the Town implement a Data Security Policy to provide guidance in the event of a data security compromise or data breach; and

**WHEREAS**, it is in the best interest of the Town of Crestone to establish a data security policy to provide general guidance on appropriate actions to be taken and documented in the event of a data security compromise or data breach that could compromise the security of the Town's sensitive information; and

**WHEREAS**, the Board of Trustees has reviewed and considered the Town of Crestone Data Security Policy, attached hereto as Exhibit A.

**NOW THEREFORE BE IT RESOLVED BY THE BOARD OF TRUSTEES OF THE TOWN OF CRESTONE, COLORADO AS FOLLOWS:**

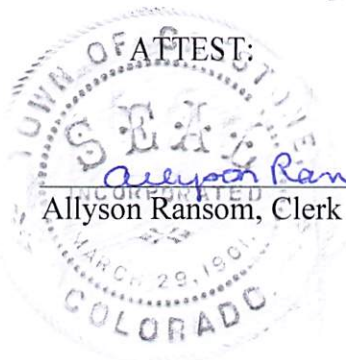
1. The Town of Crestone Security Policy attached hereto as Exhibit A is hereby adopted as the official Data Security Policy for the Town of Crestone's current and prospective employees.

**DULY MOVED, SECONDED AND ADOPTED BY THE BOARD OF TRUSTEES OF THE TOWN OF CRESTONE THIS 12th DAY OF June, 2017.**

ATTEST:

  
Allyson Ransom, Clerk

  
Kairina Danforth, Mayor



**Town of Crestone**  
**Exhibit A**  
**Data Security Policy**

**Effective Date: June 12, 2017**

**I. Purpose:**

The purpose of this Data Security Policy is to provide general guidance on the appropriate actions to be taken and documented in the event of a possible data security issue or data breach. The timeframe of the Data Security Policy ranges from the time of suspected breach to post-incident response closure, so that all incidents are handled in a consistent manner and the exposure to the potentially breached party is limited. It also provides a methodology for collecting evidence in the event of criminal activity. Documentation of responsive actions taken in connection with any data security incident or data breach, as well as documentation of the post-incident events and actions taken, is critical in making appropriate changes to business practices to improve the safeguarding and handling of the Town's sensitive information and personally identifiable information ("PII").

**II. Applicability:**

This Data Security Policy applies to all users who may experience or witness a data security incident or possible data breach. After discovery of a possible data breach, this process provides our Data Security Team with a checklist or outline for responding so that steps or information related to the incident are not missed. The Town is committed to protecting our information and responding appropriately to a data security incident or data breach.

**III. Scope:**

Protection of our information and data is paramount. This Data Security Policy provides a checklist for responding to a data security incident or potential data breach, whether intentional or unintentional, as data breach events have an adverse effect on the Town's network.

**IV. Policy/Procedures:**

This Data Security Policy describes the Town's safeguards to protect sensitive information, including PII. These safeguards:

- Protect the confidentiality, integrity and availability of data and the Town's network.
- Protect against a data breach that could result in harm or inconvenience to a resident or user and meet any notification requirements.
- Protect against anticipated threats or hazards to the security or integrity of sensitive information, including PII.
- Identify and assess the risks that may threaten PII.
- Conduct a reasonable investigation to determine the likelihood of information that has been or will be misused.
- Conduct a post-incident investigation to capture lessons learned.
- Develop written policies and procedures to manage and control these identified risks or vulnerabilities.
- Adjust the Town's network security to reflect changes in technology, the sensitivity of data stored, and internal or external threats to information security.

**V. Data Security Team:**

A Data Security Team ("DST") has been formed. This group consists of a representative from the Town's Information Technology ("IT") contractor and the Town Clerk.

## **VI. Process:**

This section establishes the steps the DST will use to respond to an incident and to initiate the Data Security Policy.

### **1. Data Security Process -Initial Discovery**

- a. In the event of a suspected or noted security incident, data breach or potential system compromise, or malicious activity, the DST shall be contacted.
- b. In order to determine if there has been a security incident, and the nature and seriousness of the incident, the DST will consider and discuss the following questions with the appropriate parties and documents the response.
  - Does the potential compromise contain Town sensitive information or PII?
  - Does law enforcement need to get involved?
  - Is there a requirement or desire to perform a forensics analysis of the system compromise?
    - o If the answer is "yes" to any of these questions then the DST will immediately coordinate actions to be taken and apply the steps c-1 below as appropriate.
    - o If the answer is "no" to all the questions, then the DST will apply the steps c-1 below as appropriate.
- c. Inform the Town Manager after DST evaluation.
- d. DST will do preliminary analysis -isolate the compromised system by disconnecting the network cable. If this is not feasible or desirable, IT can block access to the compromised system via the network.
- e. Determine the security incident type -try to determine the cause of the malicious activity and the level of system privilege attained by the intruder.
- f. Disable any compromised accounts and terminate all processes owned by them.
- g. Compile a list of IP addresses involved in the incident, including log entries if possible.
- h. Determine the users whose passwords need to be changed due to the compromise, as well as, whether or not the users have accounts on other systems using the same credentials and notify the IT administrators for those systems.
- i. Notify the owners of the compromised accounts and reissue credentials. Consider the likelihood of the intruder having access to the compromised account email and utilize other contact methodology.
- j. Determine whether all affected users have established new passwords.
- k. IT will rebuild the system and verify that its network access should be re-established.
- l. IT will perform a network vulnerability scan, if feasible and practical, of the system after it is unblocked to identify any unresolved security issues that might be used in future attacks against the system.

### **2. Post-incident Lessons Learned**

The DST will:

- a. Hold a meeting within 48 hours of completion of response.
- b. Review chronology of the event.
- c. Identify what went wrong and what went right. For instance, "Encryption was used on the file server containing Town confidential information and PII."
- d. Identify the threats or vulnerabilities that were exploited and determine whether they can be alleviated.
- e. Review if all intrusion detection or prevention was in place, active and up to date.
- f. Document "lessons learned" and assign appropriate updates to the Data Security Policy or other operational processes.

3. Privacy Breach Incident Response

If a security incident is suspected to be a data privacy breach, the DST will:

- a. Immediately notify the Town Clerk and the Town Attorney.
- b. Determine what information was suspected to be breached, i.e., specific individuals' first and last names with a type of PII.
- c. When appropriate, bring in an incident-response expert or law enforcement to conduct an investigation. Identify the scope, time frame and source(s) of breach, type of breach, whether data encryption was used and for what, possible suspects (internal or external, authorized or unauthorized, employee or non-employee user).
- d. Review for other compromised systems.
- e. Monitor all systems for potential intrusions.

**VII. Accountability:**

All users are required to report any suspected data breach of the Town's network to the DST.

The DST will respond to any incident, analyze and collect the audit records and any logs, and redeploy new credentials to affected users after identification.

IT will be responsible for maintaining updates to the Town's network security post-incident and, at a minimum, annually.

The DST will be responsible for providing the Town Attorney with documentation after an incident of the types of personal information that may have been breached, providing guidance throughout the investigation on privacy issues, and assisting in developing the communication plan to impacted individuals.

**VII. Compliance:**

Violations of this policy may lead to the suspension or revocation of system privileges and/or disciplinary action up to and including termination of employment. The Town intends to advise appropriate authorities of any violation of the law.

---

**DATA SECURITY POLICY ACKNOWLEDGMENT**

By my signature, I acknowledge that my employment with the Town of Crestone is at will and may be terminated by either party at any time. I further acknowledge that I have received a copy of the Town of Crestone Data Security Policy, have read it and understand the information contained therein. I will abide by the Policy and understand my duties, obligations and responsibilities as the same are detailed.

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Employee Name