

This information is not a substitute for legal advice, is for your reference only, and is not intended to represent the only approach to any particular issue. This information should not be construed as legal, financial or business advice, and users should consult legal counsel and subject-matter experts to be sure that the policies adopted and implemented meet the requirements unique to your company.

Office and Information Security And Privacy Policies and Program for Cass County Abstract Co., Inc.

Effective Date: June 1, 2014.

Best Practices #3: Information Security.

Risk Identification and Assessment.

All information received in this office, via any transmission or personal delivery, shall be deemed Personal Information and access to said information shall be restricted to authorized employees. Computer access to Personal Information shall be protected by password and physical access shall be contained to the employee's desk and subject to the clean desk policy as set out in the Employment Policies.

Each employee shall have a unique User ID and password for accessing technology systems, including in-house programs and sources used on the internet.

Records of the Cass County Abstract Co., Inc., shall be retained in electronic form for as long as the Company is in existence. Any documents containing Personal Information shall be shredded after archiving. Daily backups of all information shall be stored off premises.

All information received in the office shall be considered personal and the security of the employees play a vital role in properly securing data.

The Manager of Cass County Abstract Co., Inc., shall be the Privacy Officer and shall be responsible for coordinating and overseeing the Information and Security and Privacy Policy. The Privacy Officer shall be contacted to assist in providing direction and advice with security matters.

Violation of the Information Security and Privacy Policy may be subject to disciplinary action, up to and including termination of employment.

In case of emergency, employees may be authorized to access, on a per circumstance basis, secured Personal Information contained in the office's database and programs. Emergencies may include but are not limited to illness, death, fire, or natural disaster.

Review of the Office and Information Security and Privacy Policies and Program shall occur in May of every year. Any changes made shall be reviewed by the Manager and notice given to employees and Board of Directors as required. Any changes in these policies shall be noted on the old policy and retained for archival purposes.

A Customer Privacy Policy shall be delivered to each customer in June of every year by first class mail. A copy of the Policy is attached hereto as Exhibit A.

On at least a monthly basis, Cass County Abstract Co., Inc., shall review its operations to identify and assess external and internal risk(s) to the Personal Information its stores. Items to be reviewed shall include the types of Personal Information it stores, the location of that information, and how that information can be accessed by authorized and unauthorized users. Review shall include evaluating the access of each employee to the information and if any non-employees have access to that information in any manner. This review shall include all systems, and methods used for storing, processing, transmitting, and disposing of Personal Information, specifically including, but not limited to, employee training and management; information systems, including network and software design; information processing, storage and disposal; detecting preventing and responding to attacks, intrusions or other system failures. All changes required in procedures shall be made and added to these policies and reviewed with employees.

All electronic equipment and obsolete versions of software to be disposed of shall have all data destroyed before leaving the premises.

Both Internal and External Risk Management shall be done on an as-needed basis. This shall include, but not be limited to daily review of Back up Report from IT provider, emails, faxed orders, walk-in orders, telephone orders, and completed work not yet picked up by customers. These key controls shall be included in the company's risk assessment process.

If the company's employment should exceed its current employment level (one manager, one employee), key controls shall be tested by an independent party. The testing results shall be provided to the manager and the Board of Directors. If any vulnerabilities are noted, steps shall be taken to make any necessary changes so any vulnerabilities are corrected.

If a new procedure or product is added to the Company's services, it shall be added to the risk management assessments and monitored on at least a monthly basis.

Privacy Officer shall work with the IT support team to assess risks to Personal Information associated with information systems, including network and software design, information processing, and the storage, transmission and disposal of Personal Information. This shall be done on an annual basis at a minimum.

Employee Training, Management and Responsibilities

New employees and temporary contract personnel (as applicable) are provided a copy of the information Security and Privacy Policy as part of the hiring process. They are required to sign an attestation that they have read and understand the Information Security and Privacy Policy and the potential consequences of non-compliance, prior to accessing Personal Information. New employees and temporary contract personnel (as applicable) are provided their responsibilities under the Information Security and Privacy Policy as well as other application security policies and procedures, and the potential consequences of non-compliance.

Employees and temporary contract personnel (as applicable) are required to certify and re-certify if changes are made, in writing, their acceptance of the Acceptable Use of Information Technology Assets policy (e.g., acceptable use of the Internet, email, and company information resources).

Training is provided for new employees regarding the importance of information security and Personal Information during orientation that includes, but is not limited to, the proper use of computer information and passwords, control information and procedures to prevent Personal Information disclosure to unauthorized parties, and methods for proper disposal of documents containing Personal Information.

Employees and temporary contract personnel (as applicable) shall be required to repeat Information Security and Personal Information training on a periodic basis (e.g. at least annually) and shall confirm such training by signing an attestation. Successful completion and refresh of Information Security and Personal Information training shall be documented and become a part of each employees personnel file.

All training activities and documents shall be modified, as circumstances dictate, based on the risks perceived, scope and types of activities, and access to Personal Information.

Policies for termination for employees who violate the Information Security and Privacy Policy are set out in the Employee Handbook.

Retention and Destruction of Personal Information

Document retention and destruction policy is set out in the Company's Risk Identification and Assessment and includes retention time frames. All employees and contractors (as applicable) are informed of their responsibilities regarding the handling, protection and destruction of Personal Information as set out in the Employment Policies of the Company

All Personal Information is removed from equipment prior to disposal or reuse. IT contractor shall be consulted to enable the Company to perform this removal.

Any documents containing Personal Information are destroyed by shredding. The Privacy Officer regularly reviews and updates the disposal dates for all records.

Overseeing Service Providers

N/A to our Company.

Data Breach Incident Reporting

Company outsources monitoring of external threats to its network. This is accomplished by daily reporting to the Company and review of the report by the Privacy Officer. The Reports monitor and detect attacks/intrusion into systems containing Personal Information. If a breach is detected written notice shall be given to affected parties. Any breach or release, either intentional or unintentional, of Personal Information, shall be immediately reported to the Privacy Officer. A written report detailing the incident shall be made to the Privacy Officer within 12 hours of the incident's discovery. Affected parties shall be immediately notified in writing and steps shall be taken to repair the breach. Copies of all daily reports shall be retained for a period of 6 months and then shredded.

A written report form shall be available to employees, Privacy Officer, and IT contractors for use in reporting an attack/intrusion, setting out a plan to correct the problem, and steps taken to eliminate

All training activities and documents shall be modified, as circumstances dictate, based on the risks perceived, scope and types of activities, and access to Personal Information.

Disciplinary process for violation of organizational security policies and procedures by employees, temporary employees, and contractors is set out in the Employment policies handbook.

IT tools and procedures are in place and implemented as needed to reduce the risk of Personal Information disclosures whether intentional or unintentional.

CASS COUNTY ABSTRACT CO, INC., PRIVACY
POLICY

518 Chestnut Street, Atlantic, IA 50022

712-243-2136

This policy is effective from June 1, 2015.

This privacy policy sets out how **Cass County Abstract Co., Inc.**, uses and protects any information that you give Cass County Abstract Co., Inc., when you use our services.

Cass County Abstract Co., Inc., is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using services our office provides, then you can be assured that it will only be used in accordance with this privacy statement.

We may collect the following information: (1) name, company, and job title; (2) contact information including email address; (3) demographic information such as zip code and, preferences; (4) other information relevant to customer.

at we do with the information we gather: We require this information to understand your needs and provide you with better service, and in particular for the following reasons: (1) internal record keeping; (2) to improve our products and services; (3) contacting you by email, phone, fax, or mail.

We will never sell your information.

Security: We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

Cass County Abstract

CASS COUNTY ABSTRACT CO, INC., PRIVACY
POLICY

518 Chestnut Street, Atlantic, IA 50022

712-243-2136

This policy is effective from June 1, 2015.

This privacy policy sets out how **Cass County Abstract Co., Inc.**, uses and protects any information that you give Cass County Abstract Co., Inc., when you use our services.

Cass County Abstract Co., Inc., is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using services our office provides, then you can be assured that it will only be used in accordance with this privacy statement.

We may collect the following information: (1) name, company, and job title; (2) contact information including email address; (3) demographic information such as zip code and, preferences; (4) other information relevant to customer.

What we do with the information we gather: We require this information to understand your needs and provide you with better service, and in particular for the following reasons: (1) internal record keeping; (2) to improve our products and services; (3) contacting you by email, phone, fax, or mail.

We will never sell your information.

Security: We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect.

Cass County Abstract

Liability Disclaimer
for
Abstract Location Search

Cass County Abstract Co., Inc., does not provide liability insurance for the protection of individuals, groups, organizations, businesses, spectators, or others who may participate in Abstract Location Searches.

In consideration for your request of searches for location of abstracts of title, the individual, group, organization, business, or other, does hereby release and forever discharge Cass County Abstract Co., Inc., and its officers, board, and employees, jointly and severally from any and all actions, causes of actions, claims and demands for, upon or by reason of any damage, loss or injury, which hereafter may be sustained by searching for and locating abstracts.

This release extends and applies to, and also covers and includes, all unknown, unforeseen, unanticipated and unsuspected injuries, damages, loss and liability and the consequences thereof, as well as those now disclosed and known to exist. The provisions of any state, federal, local or territorial law of state providing substance that release shall not extend to claims, demands, injuries, or damages which are known or unsuspected to exist at this time, to the person executing such release, are hereby expressly waived.

I hereby agree on behalf of my heirs, executors, administrators, and assigns, to hold harmless Cass County Abstract Co., Inc., and its officers, board and employees, joint and severally from any and all actions, causes of actions, claims and demands from upon or by reason of any damage, loss or injury, which hereafter may be sustained by Cass County Abstract Co., Inc., searching for and locating abstracts.

It is further understood and agreed that said participation in locating abstracts is not to be construed as an admission of any liability and acceptance of assumption of responsibility by the Cass County Abstract Co., Inc., its officers, board, and employees, jointly and severally, for all damages and expenses for which Cass County Abstract Co., Inc., its officers, board and employees, become liable as a result of any alleged act of the participant.

Western Iowa Real Estate

Name of person signing and title

Address

Dated _____

Signature

Cass County Abstract


Business Continuity and Disaster Preparedness Plan

PLAN TO STAY IN BUSINESS

If this location is not accessible we will operate from location below:

Business Name

Business Name

Address

Address

City, State, Zip Code

City, State, Zip Code

Telephone Number

Telephone Number

The following person is our primary crisis manager and will serve as the company spokesperson in an emergency.

If the person is unable to manage the crisis, the person below will succeed in management:

Primary Emergency Contact

Secondary Emergency Contact

Telephone Number

Telephone Number

Alternative Number

Alternative Number

E-mail

E-mail

EMERGENCY CONTACT INFORMATION

Dial 9-1-1 in an Emergency

Non-Emergency Police/Fire

Insurance Provider

Business Continuity and Disaster Preparedness Plan (cont'd)

PLAN TO STAY IN BUSINESS

The following natural and man-made disasters could impact our business:

- _____
- _____
- _____
- _____

EMERGENCY PLANNING TEAM

The following people will participate in emergency planning and crisis management.

- _____
- _____
- _____
- _____
- _____

WE PLAN TO COORDINATE WITH OTHERS

The following people from neighboring businesses and our building management will participate on our emergency planning team.

- _____
- _____
- _____
- _____
- _____

OUR CRITICAL OPERATIONS

The following is a prioritized list of our critical operations, staff and procedures we need to recover from a disaster.

Operation	Staff in Charge	Action Plan
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Business Continuity and Disaster Preparedness Plan (cont'd)

SUPPLIERS AND CONTRACTORS

Company Name: _____
Street Address: _____
City: _____ State: _____ Zip Code: _____
Phone: _____ Fax: _____ E-mail: _____
Contact Name: _____ Account Number: _____
Materials / Service Provided: _____

If this company experiences a disaster, we will obtain supplies/materials from the following:

Company Name: _____
Street Address: _____
City: _____ State: _____ Zip Code: _____
Phone: _____ Fax: _____ E-mail: _____
Contact Name: _____ Account Number: _____
Materials / Service Provided: _____

If this company experiences a disaster, we will obtain supplies/materials from the following:

Company Name: _____
Street Address: _____
City: _____ State: _____ Zip Code: _____
Phone: _____ Fax: _____ E-mail: _____
Contact Name: _____ Account Number: _____
Materials / Service Provided: _____

Business Continuity and Disaster Preparedness Plan (cont'd)

EVACUATION PLAN FOR _____ LOCATION
(Insert Address)

The following natural and man-made disasters could impact our business:

- We have developed these plans in collaboration with neighboring businesses and building owners to avoid confusion or gridlock
- We have located, copied and posted building and site maps.
- Exits are clearly marked.
- We will practice evacuation procedures ____ times a year.

If we must leave the workplace quickly:

1. Warning System: _____
We will test the warning system and record results ____ times a year.

2. Assembly Site: _____

3. Assembly Site Manager & Alternate: _____
a. Responsibilities Include:

4. Shut Down Manager & Alternate: _____
a. Responsibilities Include:

5. _____ is responsible for issuing all clear.

Business Continuity and Disaster Preparedness Plan (cont'd)

SHELTER IN PLACE PLAN FOR _____ LOCATION
(Insert Address)

The following natural and man-made disasters could impact our business:

- We have talked to co-workers about which emergency supplies, if any, the company will provide in the shelter location and which supplies individuals might consider keeping in a portable kit personalized for individual needs.
- We have located, copied and posted building and site maps.
- We will practice shelter procedures ____ times a year.

If we must take shelter quickly:

1. Warning System: _____
We will test the warning system and record results ____ times a year.

2. Storm Shelter Location: _____

3. "Seal the Room" Shelter Location: _____

4. Shelter Location & Alternate : _____

a. Responsibilities Include:

5. Shut Down Manager & Alternate: _____

a. Responsibilities Include:

6. _____ is responsible for issuing all clear.

Business Continuity and Disaster Preparedness Plan (cont'd)

COMMUNICATIONS

We will communicate our emergency plans with co-workers in the following way:

In the event of a disaster we will communicate with employees in the following way:

CYBER SECURITY

To protect our computer hardware, we will:

To protect our computer software, we will:

If our computers are destroyed, we will use back-up computers at the following location:

RECORDS BACK-UP

_____ is responsible for backing up our critical records including payroll and accounting systems.

Back-up records including a copy of this plan, site maps, insurance policies, bank account records and computer back ups are stored onsite _____.

Another set of back-up records is stored at the following off-site location:

If our accounting and payroll records are destroyed, we will provide for continuity in the following ways:



Business Continuity and Disaster Preparedness Plan (cont'd)

EMPLOYEE EMERGENCY CONTACT INFORMATION

The following is a list of our co-workers and their individual emergency contact information:

_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

ANNUAL REVIEW

We will review and update this business continuity and disaster plan in _____.

Additional Notes:

Best Practices Pillar #3

Outgoing mail

Abstract storage

Personal information numbers and dates of birth

Clean Desk policy

Encrypted e-mail

Liability Disclaimer – realtors, bankers, and attorneys

Shredding

Hard drive and software disposal