eRecords
Online Document Management System

# Entity Security Policy

**Company:** _____

**Date:** _____

This form will specify how you would like the security of your eRecords entity configured. Please provide the requested information and return. Changes to this form must be submitted in writing.

## Change Authorization

Only the people listed below are authorized to make changes to this *Entity Security Policy* .

| Name | Title | Signature |
|---|---|---|
| | | |
| | | |
| | | |
| | | |

## Website Security Policy

The *Website Security Policy* specifies the twebsite security you require when accessing the system.

_____ I opt to use CRM's standard "erecords.chicagorecords.com" website. I understand that this website is encrypted using a Verisign SSL certificate which is owned and maintained by Chicago Records Management.

_____ I opt for a customized website and understand that additional charges will apply:

_____ I do not want a corporate logo of any kind on the website.

_____ I want my organizations logo on the website.

_____ I authorize CRM to purchase a SSL certificate on my behalf and bill me appropriately.

Number of years SSL certificate to be valid: _____

Prefered SSL Certificate Vendor: _____

Prefered Vendor's SSL Cert type/level: _____

Host to which SSL Cert should be assigned: _____

_____ I will provide CRM with my own SSL certificate.

## Account Lockout Policy

The *Account Lockout Policy* specifies wither or not you want User ID's disabled after a certain number of failed login attempts.

_____ Unlimited Login Attempts - Users have an unlimited number of failed login attempts to access the system.

_____ Limited Login Attempts - After a specified number of failed login attempts, User's login ID becomes disabled.

_____ Maximum number of attempts before a User ID is locked out

_____ Amount of time (in minutes) before account is automatically unlocked.
*(specify "0" if you don't want the account automatically unlocked)*

## Login Restrictions Policy

The *Login Restrictions Policy* specifies if you want your users to access the system from any IP address on the Internet, or only via IP address/subnets you specify.

_____ Allow logins from any IP address.

_____ Allow logins *only* from these specified IP address/subnets: *

_____ _____

_____ _____

_____ _____

** For administrative purposes, Chicago Records Management's subnet will also be allowed access.*

## Password Security Policy

The *Password Security Policy* defines password expiration times, minimum password length, and password complexity standards.

Password Expiration

_____ User passwords never expire.

_____ Number of days before user passwords automatically expire.

Password Length

_____ No minimum password length required.

_____ Users are forced to create passwords at least _____ characters in length.

Password Complexity (Specify "yes" or "no")

_____ Passwords must contain uppercase letters (A, B, C, D, etc.)

_____ Passwords must contain lowercase letters (a, b, c, d, etc.)

_____ Passwords must contain numeric characters (0, 1, 2, 3, etc.)

_____ Passwords must contain special characters (!, @, #, $, %, &, etc.)

**Login ID Format**

The *Login ID Format* specifies the standard CRM is to use when creating login ID's for your end users. Most any format is acceptable. Below are common examples:

Using *Steve Johnson* as an example:

| | | |
|---|---|---|
| _____ | First Initial, Full Last Name | *sjohnson* |
| _____ | Full Last Name, First Initial | *johnsons* |
| _____ | First three letters of first and last name | *stejoh* |
| _____ | First six letters last name, first initial | *johnsos* |
| _____ | Other | _____ Example |

_____ Client Signature

_____ Printed Name

_____ Title

_____ Date

_____ Chicago Records Management Signature

_____ Printed Name

_____ Title

_____ Date