CLERK OF THE COURT
SUPERIOR COURT OF ARIZONA

MARICOPA COUNTY
Downtown Justice Center
620 West Jackson, Suite 3017
Phoenix, Arizona 85003
(602) 372-5375

Department:	Clerk of the Superior Court
Division:	Strategic Planning and Information Technology
Section:	Information Technology Group (ITG)
Policy:	**BREACH NOTIFICATION**
Effective Date:	01/01/2019
L.R.D.:	
Last Reviewed Date:	

PURPOSE:

The purpose of this document is to provide Security Policy for Breach Notification in accordance with the Arizona Supreme Court Administrative Order 2018-72.

POLICY:

It is the policy of the Clerk of the Superior Court's Information Technology Group (ITG) to adhere to the points outlined in the Arizona Supreme Court's Administrative Order 2018-72, as well as A.R.S. § 44-7501, A.R.S. § 18-551, and A.R.S. § 18-552.

A.R.S. § 18-552(O) requires courts to create and maintain an information security policy that includes notification procedures for a security system breach of the court.

This policy provides direction for performing various notifications in the event of a loss of a computer or personal storage device or breach of a computer security system containing personal information as defined by A.R.S. § 44-7501 and A.R.S. § 18-551.

Responsibilities and Duties:

Court Employees:

- Any court employee who downloads all or part of a database of confidential personal information of multiple individuals to an end-user storage device, other than a court computer or court-provided mobile device, shall provide notice of a breach or suspected breach to the appropriate person in his or her chain of authority.
- End user storage devices include a personal PC, cellular phone, flash drive, or off-site data storage systems, such as web-based or cloud storage locations.

Division Directors and Managers:

- Maintain the physical security of data files containing personal information in their respective areas. This includes documenting where personal information is used and stored in each division or unit and the primary employee positions in each division or unit that have access to and use of such data.
- Ensure that all suspected security breaches within their respective division or unit are investigated and reported to the Department Head.
- Make arrangements to implement notification requirements, including the actual distribution of notification letters, emails, telephonic notices, or other substitute notice methods outlined in Arizona Supreme Court Administrative Order 2018-72, A.R.S. §44-7501, and A.R.S. §18-552.

Director of Information Technology Group (ITG):

- Provide an acceptable level of security protection for such data stored on servers.
- Facilitate the investigation of suspected security breaches resulting from unauthorized electronic access to the databases containing personal information.

Department Head (Chief Technology and Innovation Officer):

- Ensure that the Information Security Policy is followed.
- Coordinate with appropriate officials to analyze and recommend to the Clerk of Court or Chief Deputy whether a suspected security breach warrants notification.

Clerk of Court or Chief Deputy:

- Make a final determination as to whether notification of a suspected security breach is warranted.
- Notify the Presiding Judge and the Administrative Director of the Administrative Office of the Courts within 24 hours of a breach.

Notification Requirements:

- In the event of a security breach, the Clerk's Office must provide notification of the breach to those individuals whose personal information is reasonably believed to have been acquired by an unauthorized person.

- Notification must occur without unreasonable delay, except when a law enforcement agency has determined that notification will impede a criminal investigation. In this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation.

- Notification shall be provided in accordance with the methods identified in A.R.S. §44-7501(D), §18-552, and in Arizona Supreme Court Administrative Order 2018-72.

- Sample notices letters are provided in Appendix 2.

PROCEDURE:

Employees must immediately report any instance of a suspected security breach to the appropriate Division Manager, who will initiate the incident response process described below.

Initial Reporting and Analysis:

Role	Action	Timeframe/Qualifier
Authorized user	Notify immediate supervisor or Clerk's Office contact and provide details of loss, breach, or potential breach.	Immediately upon discovery.
Immediate supervisor or contact for non-employees	Notify Department Head.	Without delay.
Department Head responsible for the data impacted by the loss or breach (Chief Technology and Innovation Officer)	• Verify whether a breach or loss had occurred and scope of damage; • Notify Clerk of Court or Chief Deputy; • Notify ITG Director via cellular phone or high priority e-mail; • Notify Directors of any other agencies whose data may likely be lost or compromised; and • Notify local law enforcement agency.	Within 24 hours.
ITG Director	When appropriate, ensure assigned staff completes the	Without delay.

Role	Action	Timeframe/Qualifier
	technical analysis of the affected system to provide information to the Department Head as to whether this is an actual security breach.	
Law Enforcement	Advise Clerk of Court or Chief Deputy whether notification to affected persons would negatively impact criminal investigation.	As scope of loss is determined.

Security Breach Notification:

Role	Action	Timeframe/Qualifier

Department Head responsible for the data impacted by the loss or breach (Chief Technology and Innovation Officer)	In conjunction with appropriate Division Directors, Managers, and ITG Director: • Draft communication to affected persons using content of attached sample letters as guideline; • Mail notification to affected parties if less than 100,000 people are affected or cost of notification is less than $50,000. If more than 100,000 people are affected or cost greater than $50,000, coordinate notification through the AOC; • Determine a substitute method of notice if sufficient contact information is not available for direct hard copy or email notice; • Arrange for the logistics to implement notification; • Approve and endorse the notification communication; • Notify the Clerk of Court or Chief Deputy of the final disposition of the security breach incident, including a description of the incident, the response process, and the notification process; and • Identify actions to prevent further breaches of security.	As soon as possible once the extent of loss or breach is clearly understood and law enforcement advises investigation is not affected; and within 45 days of the positive determination of the breach, subject to the needs of law enforcement if a criminal investigation is pending.
Clerk of Court responsible for the data system that is suspected of being breached	• Shall notify the presiding judge of the court and the Administrative Director	Within 24 hours.
AOC Executive Office	• Notify State Information Security and Privacy Office at GITA; and	Without delay.

	• Communicate notice using statewide mass media outlets, if necessary.	

Large Scope Notification Instructions:

Role	Action	Timeframe/Qualifier
The Court	• The court must notify the three largest nationwide consumer reporting agencies and the Arizona Attorney General's Office as required by ARS 18-552(B)(2)(b). • The local court shall coordinate such notification through the AOC, which shall notify the public using conspicuous posting of the notice on the AZCourts.gov website for at least 45 days, and shall provide written notice to the Arizona Attorney General's Office as required by ARS 18-552(F)(4)(a).	When more than 1000 individuals are affected When the cost of individual notices exceeds $50,000 or the breach affects more than 100,000 individuals.

DEFINITIONS:

Authorized Users	All individuals approved to use Clerk of the Superior Court Technology Resources. These include Clerk employees (including temporary employees), non-employees providing services or products to the Clerk's Office (e.g., suppliers on contract) and/or non-employees who are given access to the Clerk's Office data (e.g., suppliers on contract or outside organizations.)
Breach	An unauthorized acquisition of and unauthorized access that materially compromises the security or confidentiality of

	unencrypted and un-redacted computerized personal information maintained as part of a database of personal information regarding multiple individuals.
Department Head	The Clerk of the Superior Court, Chief Deputy, Deputy Directors, Chief Technology and Innovation Officer, Director of Information Technology Group (ITG), or other members of the management team.
Division Director or Manager	The person in charge of directing the work of employees within a major component of the Clerk's Office.
Personal Information	An individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account. An individual's first name or first initial, and last name, in combination with any one or more of the following specified data elements: • Social security number; • Driver's license number or non-operating Arizona identification card number; • Private key that is unique to an individual and that is used to authenticate or sign an electronic record; • Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; • Health insurance identification number; • Information about an individual's medical or mental health treatment or diagnosis by a healthcare professional; • Passport number; • Taxpayer identification number or an identity protection personal identification number issued by the United States Internal Revenue Service; • Unique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when accessing an online account. Does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
Storage Device	Computer or computing device, including, but not limited to, servers, desktops, laptops, PDAs, removable media such as CDs, and USB flash drives used as storage devices.

APPLICABILITY:

This policy applies to all employees of the Clerk of the Court.

AUTHORIZED SIGNATURES:

Approving Authority: Issuing Authority:

Date Signed: 1-2-19

Appendix 1: Related Documents

Arizona Supreme Court Administrative Order 2008-68, which is available at: http://www.supreme.state.az.us/orders/admorder/Orders08/2008-68.pdf.

A.R.S. §44-7501, which is available at: http://www.azleg.gov/FormatDocument.asp?inDoc=/ars/44/07501.htm&Title=44&DocType=ARS.

Appendix 2: Sample Letters

SAMPLE LETTER 1

Data Acquired: Credit Card Number or Financial Account Number Only

Dear:

This letter is to inform you of a recent incident involving a breach of security for an electronic database at [name of court or department] containing [specific category of personal information].

[Describe what happened in general terms, what type of personal information was involved, and response activities underway or planned.]

To protect yourself from the possibility of identity theft, we recommend that you immediately contact the credit card or financial account issuer for the account potentially involved and ask them to either close your account or provide you with a new account number. Tell them that your account may be compromised. If you want to open a new account, ask the company to give you a PIN or password. This will help control access to the new account in the future.

For more information on identity theft, we suggest that you visit the Office of the Attorney General at http://www.azag.gov/cybercrime/ID_Theft.html; the Department of Public Safety at http://www.azvictims.com/identity/default.asp; or the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything [name of department] can do to assist you, please call [phone number].

[Closing]

SAMPLE LETTER 2
Data Acquired: Driver's License or Arizona ID Card Number

Dear:

This letter is to inform you of a recent incident involving a breach of security for an electronic database at [name of court or department] containing [specific category of personal information].

[Describe what happened in general terms, what type of personal information was involved, and response activities underway or planned.]

Since your Driver's License [or Arizona Identification Card] number was involved, we recommend that you immediately contact your local Department of Motor Vehicles office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free MVD Customer Service Center at 800-251-5866 for additional information.

If your Driver's License or Arizona ID Card Number is also your Social Security Number, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. To place a fraud alert, call any one of the three credit reporting agencies at the numbers provided below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them with instructions on how to get a free copy of your credit report.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

Look over your credit reports carefully when received for fraud evidence including the following:

- Accounts you did not open.
- Inquiries from creditors that you did not initiate.
- Personal information, such as home address and Social Security Number that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Office of the Attorney General at http://www.azag.gov/cybercrime/ID_Theft.html; the Department of Public Safety at http://www.azvictims.com/identity/default.asp; or the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything [name of your department] can do to assist you, please call [phone number].

[Closing]

SAMPLE LETTER 3
Data Acquired: Social Security Number

Dear:

This letter is to inform you a recent incident involving a breach of security for an electronic database at [*name of court or department*] containing [*specific category of personal information*].

[*Describe what happened in general terms, what type of personal information was involved, and response activities underway or planned.*]

To protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. To place a fraud alert, call any one of the three credit reporting agencies at the numbers provided below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them with instructions on how to get a free copy of your credit report.

Experian	Equifax	TransUnion
888-397-3742	800-525-6285	800-680-7289

Look over your credit reports carefully when received for fraud evidence including the following:

- Accounts you did not open.
- Inquiries from creditors that you did not initiate.
- Personal information, such as home address and Social Security Number that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports every three months for the next year. Call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you visit the Office of the Attorney General at http://www.azag.gov/cybercrime/ID_Theft.html; the Department of Public Safety at http://www.azvictims.com/identity/default.asp; or the Federal Trade Commission at www.consumer.gov/idtheft. If there is anything [*name of your department*] can do to assist you, please call [*phone number*].

[*Closing*]