Print Clear

Attorney Name: _____
Attorney ID: _____
Address:_____
Email:_____
Phone: _____

Certification of Attorney Regarding Cybersecurity Incident and Request for Restoration of Access to New Jersey State Judiciary Systems

In Re Cybersecurity Incident Involving _____(Attorney/Firm) on _____(Date).

CERTIFICATION

I, _____ (attorney name, attorney ID: _____), an attorney at law of the State of New Jersey hereby certify as follows:

1. I am a New Jersey attorney in good standing with _____ (firm name).
2. ☐ I am a solo practitioner.

   ☐ I am associated with the law firm of _____.
3. On _____ (date of incident), I discovered or was alerted about a confirmed or potential cybersecurity incident or breach, which I understand to involve the following risks: (select all that apply)

   ☐ Phishing attempt

   ☐ Malware link

   ☐ Ransomware

   ☐ Other: _____

   ☐ Unknown
4. The following users are affected by the incident. (Include attorney IDs for all attorney users and approved designees. Attach a list, if necessary).
5. The following email addresses are associated or otherwise implicated by this cybersecurity incident (please list all email addresses, including those used by a designee as well as any personal email addresses and/or provide the domain address for all affected users):

   _____
6. (a) My office's email accounts are managed through _____(email provider).

   (b) My office's email accounts have the following application add-ons, such as Microsoft 365 with Microsoft Outlook, if known: _____.

7. (select all that apply):

   ☐ Upon discovering or being alerted to the cybersecurity incident, I contacted the Superior Court Clerk's Office to report the situation.

   ☐ I reported the cybersecurity incident to _____ (other agencies, such as the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC), New Jersey State Police).

   ☐ I was contacted by the New Jersey Judiciary on _____ (date) regarding this incident.

8. I understand that all emails from the above-listed affected email addresses were quarantined, and access to Judiciary accounts was suspended for all users, consistent with Judiciary Administrative Directive #11-23 ("Responding to Information Security Incidents, Including Compromised Attorney Accounts").

9. As directed by the Superior Court Clerk's Office, I am submitting this certification that sets out steps that have been taken in response to this incident, as well as additional measures that have been implemented to prevent such cybersecurity incidents from occurring in the future.

Response to and Remediation of This Incident

10. The account passwords for all affected users and email addresses have been reset and changed. Strong, unique passwords are being used by all users and all email addresses.

11. All malicious software, unauthorized access points, and compromised credentials were removed. Any system vulnerabilities were patched, and any compromised accounts were reset.

12. Password changes were implemented using a different device than the devices to which the emails are assigned and traditionally accessed and managed. After making the changes, all accounts were signed out and then reopened. [Add further explanation, if needed.]

Prevention of Future Incidents

13. Multi-factor authentication has been enabled as a mandatory feature of all affected accounts and any other accounts associated with my practice. [Add further explanation if applicable, including as to the installation of an authenticator application on other devices.]

14. Consistent with cybersecurity best practices, a full scan (using _____ software) has been completed as to all affected devices.

    ☐ This scan has revealed no unresolved vulnerabilities. **Or**

    ☐ This scan revealed the following vulnerabilities:_____ (such as, a rule had been created and applied in mail settings, which was causing incoming emails to be redirected to another account). Those vulnerabilities have been resolved, (such as the rule has been deleted).

15. Advanced threat detection software and 24/7 monitoring has been implemented (using _____ software) in order to be able to detect and respond to future threats more quickly.

16. Indicate any additional measures taken (select any/all that apply):

- ☐ All employees have participated in mandatory cybersecurity training, focusing on phishing awareness, password management, and identifying suspicious activities.
- ☐ Attorney users have enrolled or will enroll in relevant continuing legal education programs on cybersecurity threats.
- ☐ Internal cybersecurity policies and incident response procedures have been revised to align with best practices.
- ☐ Periodic security audits and penetration testing has been scheduled to identify and remediate vulnerabilities proactively.
- ☐ Relevant reports are attached (from an IT consultant or cybersecurity consultant).
- ☐ Other: _____
- ☐ None

Request for Reinstatement of Access

17. At this point, I request restoration of access to New Jersey Judiciary electronic systems for all affected users and email addresses, as set forth above.

18. I understand that I am required to promptly report any future cybersecurity incidents to the New Jersey Courts by calling the Superior Court Clerk's Office.

19. I certify that the foregoing statements made by me are true. I am aware that if any statements are willfully false, I am subject to punishment.

_____ s/_____

Date Attorney's Signature

Name
Attorney ID:
Address:
Email:
Phone: