CYBER INCIDENT PROCEDURE AND EMERGENCY CONTACTS

Identify, contain and eliminate

STEP 1 – IDENTIFY: CONFIRM AND CATEGORISE THE CYBER INCIDENT

STEP 2 – CONTAIN: REPORT THE CYBER INCIDENT

IF MONEY HAS GONE MISSING

Immediately notify:

1. Your bank's fraud team on
   _____
2. Lawcover Group Cyber Policy Response Team on 1800 4 BREACH (1800 427 322)
3. If trust money involved, the Law Society of NSW's Trust Accounts Department on (02) 9926 0337.

Then report the incident to:

4. Your IT service provider on
   _____
5. Australian Cyber Security Centre (cyber.gov.au)
6. ACCC Scamwatch (scamwatch.gov.au)
7. If required, Office of the Australian Information Commissioner (oaic.gov.au)
8. Disconnect any affected system from the network, if you are sure that it is safe to do so (do not turn systems off or otherwise interfere with systems as this may hamper any investigation effort)

IF INCIDENT DOES NOT INVOLVE MISSING FUNDS

Report the incident to:

1. Lawcover Group Cyber Policy Response Team on 1800 4 BREACH (1800 427 322)
2. Your IT service provider on
   _____
3. Australian Cyber Security Centre (cyber.gov.au)
4. ACCC Scamwatch (scamwatch.gov.au)
5. If required, Office of the Australian Information Commissioner (oaic.gov.au)
6. Disconnect any affected system from the network, if you are sure that it is safe to do so (do not turn systems off or otherwise interfere with systems as this may hamper any investigation effort)

STEP 3 – ELIMINATE: POST EVENT EVALUATION

1. Identify lessons learned and implement improvements to cyber security system
2. Review your cyber security response plan for effectiveness
3. Continue staff training

Lawcover

THE LAW SOCIETY OF NEW SOUTH WALES

LS4016