

Incident Type	Number	Description/Examples
Data spill via email	13	Unintentional and unauthorised release of information via email (usually staff accidentally including the wrong email address, or personal email address)
Loss of equipment	2	Loss of ACIC assets
Loss/theft of access pass	4	Loss of ACIC Security Pass, or ACIC Credentials
Password/account sharing	1	Staff sharing or providing other staff access to their account, software or systems
Prohibited item in secure area	1	Typically, staff unintentionally taking a phone, smart watch or USB into the SCIF
Suspicious activity	6	Members of the public loitering outside of ACIC premises, conduct by a staff member which is out of character or unusual (excessive printing, working unusual hours)
Suspicious contact	5	Unsolicited contact with an ACIC staff member by a member of the public who is a person of interest or target of the ACIC
Unauthorised access to premises	1	Typically, member of the public tailgating ACIC staff into ACIC car parks, members of the public making their way to secure floors (into the foyer), staff who attempt to access ACIC premises after-hours when not authorised
Unauthorised disclosure	5	Unauthorised release of ACIC information (as per ACC Act) by any means (deliberate or unintentional)
Unsecure container	2	Container not locked or appropriately secured
Unsolicited contact	4	Member of the public contacting or approaching an ACIC staff member via phone, mail, email or in person. Typically asking for staff members by name or knowing who they are and where they work
Visitor not signed in/escorted	1	