

APPENDIX “B”

INFORMATION SECURITY INCIDENT LEVELS AND ADVANCED TECHNOLOGY RESPONSE SUMMARY

Incident severity classifications described below are used as guidelines. If there is doubt about the classification of an Information Security Incident, the higher severity classification should be used as a precautionary measure. Inquiries about the IT Security Office response to an Incident should be directed to the IT Security Office.

LOW CRITICALITY INCIDENTS

Activity Examples	<ul style="list-style-type: none"> • detected unsuccessful denial of service, or unsuccessful distributed denial of service attempts (blocked at firewall/router); • incidental unsuccessful access attempts either from within or outside Region’s network; • potential for penetration of IT infrastructure detected or unauthorized access suspected; • instances of known computer viruses or worms are detected and successfully contained or removed by deployed anti-virus or other installed software; • abuse of IT Resources, User privileges, or password confidentiality, not extending to superuser, root or administrator privileges. 	
Potential Outcome	<ul style="list-style-type: none"> • low potential for disruption to IT Resources or services (e.g., not widespread); • low legal risk; or • otherwise low-level threat. 	
Who	Task	Response Time
Staff/Manager	1. Staff reports the Incident to the Supervisor/Manager	Within 24 hours
	2. Supervisor/Manager reports to IT Help Desk.	Immediately
IT Help Desk	3. IT Help Desk reports to IT-security@calgaryhealthregion.ca .	Less than 2 business days
All	4. The IT Security Office investigates, makes recommendations, implements preventative measures, and notifies the I&P Office if there is a potential privacy breach.	
Maximum Total Response Time: 2 business days		

MEDIUM CRITICALITY INCIDENTS

Activity Examples	<ul style="list-style-type: none"> • stolen or missing IT equipment without Information capabilities; • sensitive Information is acquired by unauthorized individual, or unauthorized access to any account, at any access level; • repeated active probes or port-mapping from an external network; • isolated case of suspected or confirmed identify theft; • abuse of IT Resources, User privileges, or password confidentiality, extending to superuser, root, or administrator privileges; • detection of a physical intrusion into secure IT facilities; or • multiple recurrence of low criticality activities. 	
Potential Outcome	<ul style="list-style-type: none"> • moderate disruption to IT Resources or services, or business continuity disruption; • substantial harm to an individual’s privacy or the Region’s credibility; or • serious risk of legal action or potential legal issues. 	
Who	Task	Response Time
Staff/Manager	1. Staff reports the Incident to the Supervisor/Manager.	Within 12 hours
	2. Supervisor/Manager reports to IT Help Desk.	Immediately
IT Help Desk	3. IT Help Desk reports to IT-security@calgaryhealthregion.ca .	Less than 2 business days
All	4. The IT Security Office investigates, makes recommendations, implements preventative measures, and notifies the I&P Office if there is a potential privacy breach.	
Maximum Total Response Time: 2 business days		

APPENDIX “B” cont’d

HIGH CRITICALITY INCIDENTS

Activity Examples	<ul style="list-style-type: none"> • stolen or missing IT equipment with Information capabilities; • widespread virus or worm infection (over 10% of hosts) not managed by standard anti-virus software; • high- or extreme-sensitive Information is acquired by an unauthorized individual; • IT systems actively attacking other systems (internal or external); • successful attack against system services (e.g., DNS, e-mail, www, denial of service attack); • unavailability of mission critical systems or applications; or • multiple recurrences of medium criticality activities. 	
Potential Outcome	<ul style="list-style-type: none"> • severe disruption to the Region’s IT Resources or services; • business continuity disrupted; • substantial harm to individual privacy and/or the Region’s credibility; or • interference with civil or criminal justice administration. 	
Who	Task	Response Time
Staff/Manager	1. Staff reports the Incident to the Supervisor/Manager.	Immediately
	2. Supervisor/Manager reports to IT Help Desk immediately.	Immediately
IT Help Desk	3. IT Help Desk reports to ITsecurity@calgaryhealthregion.ca .	Same day
ALL	4. The IT Security Office investigates, makes recommendations, implements preventative measures, and notifies the I&P Office if there is a potential privacy breach.	
Maximum Total Response Time: Same day		