

## APPENDIX “C”

### INFORMATION SECURITY INCIDENT LEVELS AND I&P OFFICE RESPONSE SUMMARY

*In assigning the severity level, the Information and Privacy (I&P) Office shall take into account factors including but not limited to the Security Classification (Appendix “A”), any relationship between the subject and recipient of the Information, any evidence of staff misconduct or negligence, or media involvement. **Inquiries regarding the I&P Office response to an Incident should be directed to the I&P Office.***

#### LEVEL 1 INCIDENTS

<b>Potential Outcomes</b>	<ul style="list-style-type: none"> <li>• minimal harm to individual privacy; or</li> <li>• minimal harm to the Region’s credibility</li> </ul>	
<b>Potential Disciplinary Action</b>	<ul style="list-style-type: none"> <li>• additional training;</li> <li>• verbal warning;</li> <li>• more serious discipline that may include termination for repeated Information Security Incidents.</li> </ul>	
<b>Who</b>	<b>Task</b>	<b>Response Time</b>
<b>Staff/Manager</b>	1. User or manager reports the Incident immediately to the I&P Office, retrieves the Information as soon as possible, and takes actions to limit the harm caused. Information may be retrieved in person or by courier.	Immediately
<b>I&amp;P Office</b>	2. The I&P Office investigates the Incident for causes and takes further steps to mitigate potential damages. Responsible staff, and manager cooperate with the investigation, as required.	Less than 20 business days
	3. The I&P Office compiles a report of recommendations and preventative measures. The report is sent to the responsible Manager/Director.	
<b>Maximum Total Response Time: 20 business days</b>		

#### LEVEL 2 INCIDENTS

<b>Potential Outcomes</b>	<ul style="list-style-type: none"> <li>• harm to individual privacy; or</li> <li>• harm to the Region’s credibility.</li> </ul>	
<b>Potential Disciplinary Action</b>	<ul style="list-style-type: none"> <li>• immediately placed on leave (with pay);</li> <li>• additional training;</li> <li>• verbal or written warning; or</li> <li>• more serious discipline that may include termination for repeated breaches.</li> </ul>	
<b>Who</b>	<b>Task</b>	<b>Response Time</b>
<b>Staff/Manager</b>	1. User or manager reports the Incident immediately to the I&P Office, retrieves the Information as soon as possible, and takes action to limit the harm caused. Information may be retrieved in person or by a courier.	Immediately
<b>I&amp;P Office</b>	2. The I&P Office investigates the Incident for causes and takes further steps to mitigate potential damages. Responsible staff and manager cooperate with the investigation, as required.	Less than 20 business days
	3. The I&P Office compiles a report of recommendations and preventative measures. The report is sent to the responsible Manager/Director.	
<b>Maximum Total Response Time: 20 business days</b>		

## APPENDIX “C” Cont’d

### LEVEL 3 INCIDENTS

<b>Potential Outcomes</b>	<ul style="list-style-type: none"> <li>• serious harm to individual privacy;</li> <li>• serious harm to the Region’s credibility;</li> <li>• risk to Region disaster preparedness and recovery;</li> <li>• substantial economic harm to third parties or the Region; or</li> <li>• serious risk of legal action against the Region.</li> </ul>	
<b>Potential Disciplinary Action</b>	<ul style="list-style-type: none"> <li>• immediately placed on leave (with pay);</li> <li>• investigation; or</li> <li>• upon confirmation of responsibility for the Incident, disciplinary action which may include termination and possible legal action.</li> </ul>	
<b>Who</b>	<b>Task</b>	<b>Response Time</b>
<b>Staff/Manager</b>	1. User or manager reports the Incident immediately to the I&P Office, retrieves the Information as soon as possible, and takes action to limit the harm caused. Information may be retrieved in person or by courier.	Immediately
<b>I&amp;P Office</b>	2. The I&P Office investigates the Incident for causes and takes further steps to mitigate potential damages. Responsible staff, manager, and Executive cooperate with the investigation, as required.	Less than 10 business days
	3. The I&P Office compiles a report of recommendations and preventative measures. The report is sent to the responsible Manager/Director, Executive Director, Medical Director, and the Information Security Group, as appropriate.	
<b>Maximum Total Response Time: 10 business days</b>		

### LEVEL 4 INCIDENTS

<b>Potential Outcomes</b>	<ul style="list-style-type: none"> <li>• serious harm to individual privacy;</li> <li>• serious harm to the Region’s credibility;</li> <li>• risk to Region disaster preparedness and recovery;</li> <li>• substantial economic harm to third parties or the Region; or</li> <li>• serious risk of legal action against the Region.</li> </ul>	
<b>Potential Disciplinary Action</b>	<ul style="list-style-type: none"> <li>• immediately placed on leave (with pay);</li> <li>• investigation; or</li> <li>• upon confirmation of responsibility for the Incident, disciplinary action which may include termination and possible legal action.</li> </ul>	
<b>Who</b>	<b>Task</b>	<b>Response Time</b>
<b>Staff/Manager</b>	1. User or manager reports the incident immediately to the I&P Office, retrieves the Information as soon as possible, and takes action to limit the harm caused. Information may be retrieved in person or by courier.	Immediately
<b>I&amp;P Office</b>	2. The I&P Office investigates the Incident for causes and takes further steps to mitigate potential damages. Responsible staff, manager, and Executive cooperate with the investigation, as required.	Less than 10 business days
	3. The I&P Office compiles a report of recommendations and preventative measures. The report is sent to the responsible Manager/Director, Executive Director, Medical Director, and the Information Security Group, as appropriate.	
<b>Maximum Total Response Time: 10 business days</b>		