Incident Number	Reported Date/Time	Summary	Organizational Rollups.Ministry
2019-000241	2019-Feb-01	As reported, on March 13th, 2018 a Freedom of Information (FOI) Request was uploaded to the government's Open Information website which contained unredacted applicant information in a password letter. The breach was noticed on February 1st, 2019, and upon further investigation, another FOI request which had been uploaded to the Open Information website on May 30th, 2018 was also found to contain unredacted applicant information. Both requests were made by the same applicant and were made for general government information. Personal information disclosed included the applicants name, address, and the fact that they had made these freedom of information requests. On February 1, 2019, the files were taken down from the Open Information website. Containment has been achieved.	Citizens' Services
2019-000246	2019-Feb-01	As reported on February 1, 2019, four government issued computers were reported missing while conducting a recent inventory. It is unknown whether these computers were locked or password protected. It is unknown what kind of personal or confidential information may have been on them. OCIO Security confirmed all four computers were encrypted. As such, no further containment measures are necessary.	Citizens' Services
2019-000286	2019-Feb-07	An email was sent to 120 businesses regarding an application change. The email addresses were inadvertently placed in the CC field instead of the BCC field.	Citizens' Services
2019-000303	2019-Feb-11	It was recently discovered that in July 2017, a FOI response package involving records from the Ministry of Transportation and Infrastructure was provided to a third party which contained information considered to be protected by solicitor-client privilege. It was confirmed by legal counsel that the one page document included in the package should have been severed under section 14 of the Freedom of Information and Protection of Privacy Act.	Citizens' Services
2019-000313	2019-Feb-12	As reported, the Complainant alleges that managerial staff obtained medical information from the Public Service Agency without appropriate authorization.	Citizens' Services
2019-000332	2019-Feb-14	As reported, an email was sent to four recipients confirming their success moving forward in a hiring competition. The four recipient email addresses were in the CC field instead of the BCC field. The personal information involved includes four email addresses which contain the first and last name of each recipient. All four recipients confirmed double deletion of the email. Containment was achieved.	Citizens' Services
2019-000349	2019-Feb-15	As reported, the Complainant alleges that information regarding an assault was inappropriately shared with executive-level management staff. The Complainant further alleges that her personal information, including details related to her work history, was volunteered by PSA and a Ministry executive to the police unnecessarily.	Citizens' Services

Incident Number	Reported Date/Time	Summary	Organizational Rollups.Ministry
2019-000354	2019-Feb-19	A computer has been deemed missing while conducting a recent inventory. The computer is believed to have been returned 2 refreshes (approximately 6 years) ago but is still on the Branch's asset list so it may have been misplaced. It is unknown what kind of personal or confidential information may have been on the computer, though the employees in the branch don't often deal with personal information.	Citizens' Services
2019-000383	2019-Feb-22	Due to routing error within MyService Now, this is a double count of file 2019-0313.	Citizens' Services
2019-000392	2019-Feb-25	Employee A, who is currently in the hospital and on extended leave, provided their IDIR login details to Employee B for the purposes of an accessing required business information that is saved in Employee A's Outlook mailbox. The login information was written on a piece of paper, but Employee B indicates they did not utilize the credentials and did not access Employee A's information. The piece of paper with Employee A's IDIR login credentials written on it has been destroyed.	Citizens' Services
2019-000416	2019-Feb-28	As reported, a laptop belonging to Employee A was taken by Employee B without prior approval. The laptop was with Employee B for approximately 45 minutes.	Citizens' Services
2019-000417	2019-Feb-28	It was discovered on February 27, 2019, that an address was disclosed in a letter posted on Open Information. The individual's name was removed but the address was left in error. The document has been removed from the site and corrected. s.13 s.13	Citizens' Services
2019-000421	2019-Feb-28	*Double report*As reported, a laptop belonging to Employee A was taken by Employee B. Confirmation that the laptop was secured with a strong password, that the user's IDIR and password were not written down on or near the device, and that the device is encrypted is currently being sought. At this time it is unknown the purpose for which the laptop was taken or for how long Employee B had the device in their possession.	Citizens' Services
2019-000428	2019-Feb-28	A message was sent to Employee A via Skype for Business. It was discovered that a second recipient was added to the conversation without their approval. The message included the first name of three employees and discusses temporary assignment backfill approval. The sender contacted the unintended recipient who confirmed they never received the message.	Citizens' Services