PR IT'S cyber security

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

CYBERSECURITY

INCIDENT REPORT

Guideline

For the Executive Branch of the Government of Puerto Rico

As established by the Puerto Rico Innovation and Technology Service by virtue Act 75-2019

Table of Contents

Introduction

By virtue of Act 75-2019, the Puerto Rico Innovation and Technology Service (PRITS) was created to establish and promote public policy on the preparation, management, development, coordination, and effective interagency integration of innovation and technological infrastructure and information technology of the Government of Puerto Rico. The PRITS responsibilities include the development of a cybersecurity framework and establish and implement the policies, applications, processes, and procedures that guarantee effective government security controls for information systems, electronic files, the use of the internet, and the interagency network.

To capture the critical information related to cybersecurity incidents, the PRITS has developed a Cybersecurity Incident Report section in the PRITS ServiceDesk tool. It will allow users to inform and document all cybersecurity events that have resulted in an incident that represents a violation of laws, security procedures and policies, or is a threat or has put a risk to the Government information or information systems. This report will be essential to gather relevant information for further analysis based on the provided historical data, activities that are taking place, involved parties, and future action plans.

Definitions

For this reporting guideline, the following terms shall have the meaning set forth below:

1. *Agency* – Means any board, body, examining board, commission, public corporation, office, division, administration, bureau, department, authority, official, employee, person, entity, or any instrumentality of the Executive Branch of the Government of Puerto Rico.

2. *Data breach* – means the loss of control, compromise, unauthorized disclosure and/or acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses Personally Identifiable Information (PII) or Protected Health Information (PHI), or an authorized user accesses PII or PHI for another than authorized purposes.

3. *Government* – Means the Government of Puerto Rico.

4. *Incident* – means any occurrence that (i) actually or imminently put at risk, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (ii) represents a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

5. *Information integrity* – means guarding against improper information modification or destruction, and ensuring information nonrepudiation and authenticity.

6. *Information resources* – means information and related resources, such as personnel, equipment, fund, and information technology.

7. *Information security* – means protecting information and information systems from unauthorized access, utilization, disclosure, disruption, modification, or destruction to provide (i) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; (ii) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; and (iii) availability, which means ensuring timely and reliable access to and use of information.

8. *Information system* – means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

9. *Loss or theft of device or media* – occurs when an employee, contractor, or other authorized individual loses possession, through misplacement or wrongful appropriation by someone, of a government's information technology equipment, device, or media that can be used to access sensitive data, the government network, accounts, or may pose a threat to information security.

10. *Malicious code* (ransomware/malware/virus/worms) – means an arbitrary group of letters, numbers, or symbols organized as a set of instructions for a computer that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

11. *Office 365 compromised account* – occurs when someone steals or has unauthorized access to the Office 365 credentials (e.g., name, password, or PIN).

12. *Personal Identifiable Information* (PII) – means any representation of information that is readable without the need of a special cryptographic key to access it, allows or facilitates tracing an individual's identity, includes the name or first initial and the paternal surname of an individual combined with other information, and that is linked or linkable to a specific individual such as:

    (a) Social Security Number
    (b) Driver's license number, voter's ID or credentials, or any other official identification
    (c) Bank or financial account numbers of any kind, with or without access codes that may have been assigned
    (d) Username and passwords to access public or private information systems
    (e) Medical information protected by the Health Insurance Portability and Accountability Act (HIPAA)
    (f) Taxpayer information
    (g) Job evaluations

13. *Protected Health Information (PHI)* – means any representation of information that is readable without the need of a special cryptographic key to access it, contains at least an individual's name or first initial,

and the paternal surname combined with medical information protected by the Health Insurance Portability and Accountability Act (HIPAA), including, demographic information, medical history, test and laboratory results, mental health conditions, insurance information, or any other data healthcare professionals collect to identify an individual and determine appropriate care.

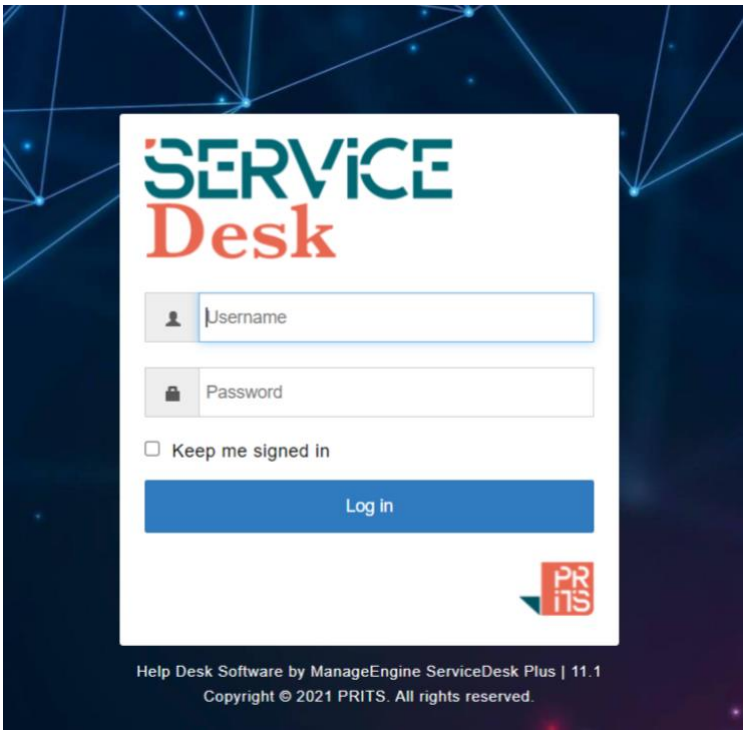
14. *PRITS* – Means the Puerto Rico Innovation and Technology Service.

15. *Social Engineering (phishing/spoofing/vishing/other)* – means the act or attempt to trick or deceive an individual into revealing sensitive information (e.g., password) or performing certain actions that can be used to obtain unauthorized access, commit fraud, attack systems or networks, download and execute files that appear to be benign but are in fact malicious, among others.

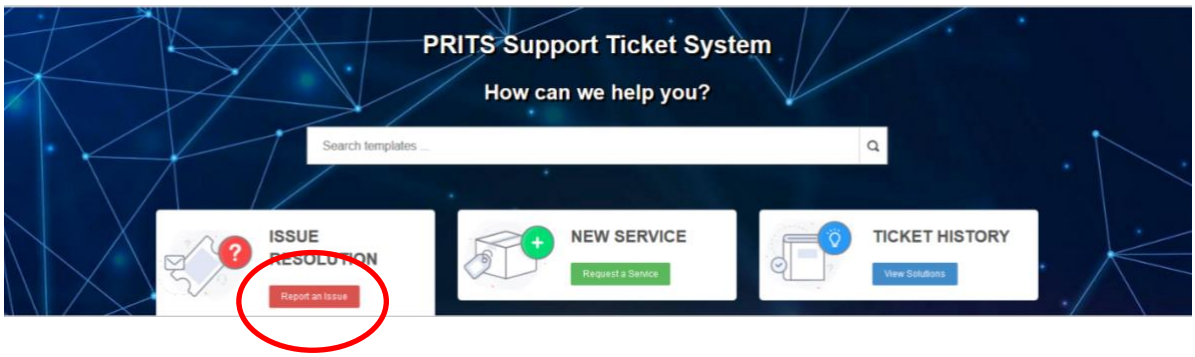
16. *Unauthorized access* / *Hacking* – occurs when a person gains logical or physical access without approval or consent to a network, system, data, application, or other information technology resource.

Instructions

1. Please login to your ServiceDesk user account using the link support.prits.pr.gov

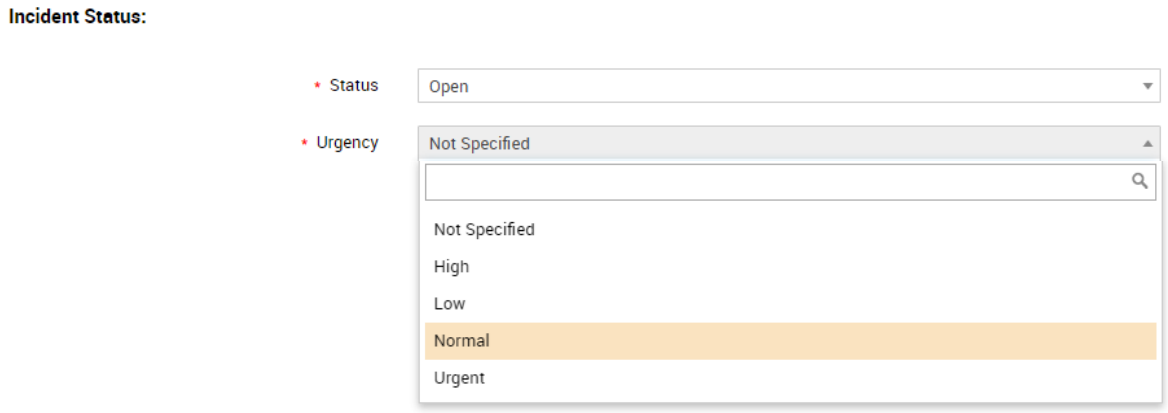


2. Click *Report an Issue*.



3. Select the option *Cybersecurity Incident Report*.

4. Under the section *Incident Status* section, please select the urgency of the incident.



Urgency is based on the following criteria:

(a) *Low*
The incident has little or no impact or affects only a few users.

(b) *Normal*
The incident has minor effects on a small group of users, does not cause the interruption of services, or poses little threat to data or network security.

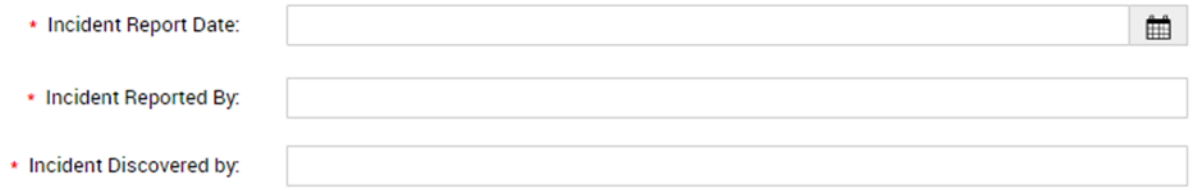
(c) *High*
The incident is likely to impact a small group of users, interrupt non-essential services, and involves data or network security breaches.

(d) *Urgent*
The incident is causing the degradation of vital service(s) for a large number of users, constitutes a serious breach of network security or data, affect mission-critical equipment or services, or damage public confidence in the agency.

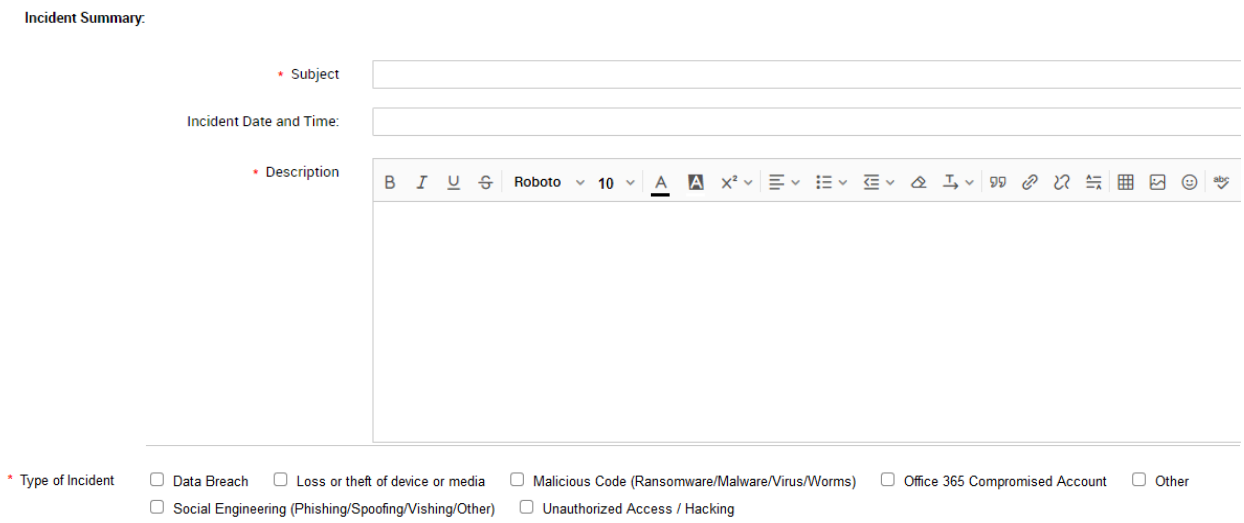
5. In the *Contact Information* section, please include (a) the name and phone number of the agency point of contact in charge of the cybersecurity; and (b) the date on which the incident was reported, the name of the person that reported it, and the name of the person that discovered the incident.

(a)

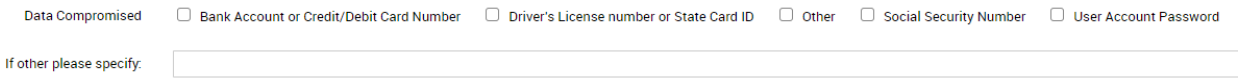
(b)



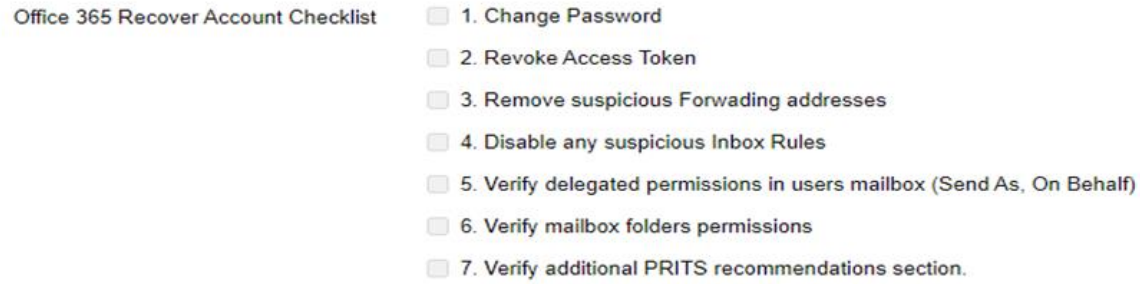
6. In the *Incident Summary* section, enter the incident subject, the description of the event, the date and hour in which it occurred (if available), and the type of incident.



(a) If the incident type was a *Data Breach,* then fill in the *Data Compromised* section and select the type of data that is suspected to have been affected. If the data compromised is not presented in the options, please specify in the space provided.



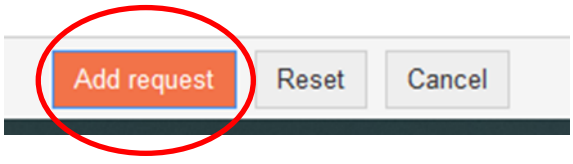
(b) If the incident type was an Office 365 Compromised Account, go through the Office 365 Recovery Account Checklist. Check the boxes corresponding to the steps that have been already completed. For more details on these steps, refer to the document "Proceso de respuesta a incidentes: buzones de cuentas comprometidas de usuario Office 365".



7. In the *Additional Information* section, include any available supplementary information. If it is not available, the spaces can be left blank.

8. To support the documentation of the incident, additional files or screenshots can be enclosed in the *Attachments* section.

9. To complete the incident reporting process, click *Add request*.



Document Maintenance

The Chief Innovation & Information Officer (CIIO) of the Government of Puerto Rico, or its designated personnel, will have the authority to make any changes to this document. This guideline shall be reviewed periodically, as technology and innovation procedures evolve. Recurrent short and medium-term revisions might be expected as the PRITS continue to incorporate requirements and refine the criteria based on (1) best practices and recognized standards, (2) the integration of tools to optimize the process, and (3) as users' feedback is analyzed and addressed.

Revision History

Date	*Description of Change*	*Approved by*
8/30/21	Initial Version	Nannette Martínez, CTO