IT Security Incident Management Policy

IT Security Incident Management Policy			
Effective Date	June 27, 2016	**Cross- Reference**	1. IT Operations and Maintenance Policy 2. Record Classification and Handling Policy
Policy Holder	Director, Information Technology		
Approver	Executive Council		
Review Schedule	Every 5 years	**Appendices**	1. IT Security Incident Reaction Plans

1. Policy Statement

1.1 Whether it is a leak of students' personal information or the disruption of the network due to a malware contamination, the impact to Grande Prairie Regional College ("GPRC", or "the Institution") reputation and financial costs to recover from an information security incident can quickly escalate.

1.2 The Institution must have preventative controls as well as reactive procedures in place to minimize the risk and impact of incidents and to effectively address such occurrences.

2. Background

2.1 All information security incidents, actual or suspected, must be reported, documented, assessed, mitigated and communicated as appropriate.

2.2 Detection controls, including procedures and tools must be in place to detect and escalate as soon as possible any occurrence of a security incident.

2.3 When occurring, security incidents must be effectively addressed to contain and mitigate negative impacts and return to a normal situation in a timely manner.

3. Policy Objective

3.1 The objective of this policy is to ensure the Institution has reasonable security controls in place to prevent, detect and address information security incidents.

4. Scope

4.1 This policy applies to:

4.1.1 All GPRC offices, campuses and learning centres

4.1.2 All students, employees, consultants, contractors, agents and authorized users accessing GPRC IT systems and applications

4.1.3 All IT systems or applications managed by GPRC that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems

5. Definitions

5.1 "Information Security Incidents" are unplanned events which affect the confidentiality and integrity of data and the availability of IT systems. Examples of an information security incident include: confidential data breach, privacy breach, unauthorized access to applications and network, malware contamination, web site defacement, etc. Security incidents that have a high probability of being exploited and that will highly impact the Institution (i.e. risk of operation disruption, data breach, etc.) are often labeled as "Critical" or "High".

5.2 "Critical Security Incidents" are security incidents that present the highest probability of being exploited and that have a high impact to the Institution.

5.3 "Users" are persons accessing an IT system or application.

6. Guiding Principles – General Requirements

6.1 All users must immediately report any observed or suspected event that potentially presents a security risk or is in violation of GPRC security policies, such as:

6.1.1 Suspicious behaviour of a GPRC system or application

6.1.2 Suspicious behaviour of a user

6.1.3 Security weakness in GPRC technology, systems or services

6.2 When an information security incident occurs, the IT Help Desk must be immediately informed. The IT Help Desk is the first point of contact for such incident.

6.3 GPRC will take appropriate actions in response to information security incidents to:

6.3.1 Immediately contain the information security incident and prevent any further impact where possible

6.3.2 Remediate the incident and return to a normal situation in a timely manner

6.3.3 Communicate internally with stakeholders impacted by the incident, as well as with necessary stakeholders to contain and remediate the incident

6.3.4 Communicate with external stakeholders, including the public, students, business partners and law enforcement authorities, where applicable

6.3.5 Document in a formal incident report the details of the incident, including:

6.3.5.1 Timeline of the information security incident

6.3.5.2 How the incident was detected

6.3.5.3 How the incident occurred, and if any gap in the security controls in place facilitated the occurrence of the incident

6.3.5.4 The impact of the incident (e.g. as cost to remediate and loss of data)

6.3.5.5 How the incident was contained and remediated

6.3.5.6 The lessons learned from the incident, to prevent the re-occurrence of such an incident in the future

6.4 Appendix 1 contains reaction plans for a number of specific security incident scenarios.

6.5 The Institution will maintain and regularly update incident response plans for common security threats.

6.6 Operational procedures must be maintained and regularly reviewed for the operation of security and system monitoring services, such as:

6.6.1 Security log monitoring and Security Information and Events Management (SIEM)

6.6.2 Intrusion Detection and Prevention systems (IDS/IPS)

6.6.3 Network firewalls

6.6.4 Web application firewalls

6.6.5 Anti-malware software

6.6.6 Email and web filtering systems

6.6.7 Network performance monitoring tools

6.6.8 Procedures and tools to monitoring the usage of GPRC technology (such as network, email, web access and applications)

7. Roles and Responsibilities

STAKEHOLDER	RESPONSIBILITIES
Executive Council	• Approve and formally support this policy
Vice-President, Administration	• Review and formally support this policy
IT Director	• Develop and maintain this policy • Review and approve the incident reaction plans as well as the security monitoring procedures • Review and approve any exceptions to the requirements of this policy • Takes proactive steps to reinforce compliance of all stakeholders with this policy
Supervisors or Institution Representative	• Support all employees and students in the understanding of the requirements of this policy • Immediately assess and report to the IT service desk any non-compliance instance with this policy
Contract Manager	• Ensure that the responsibilities and obligations of each party to the contractual relationship are outlined in the contract executed between the Institution and the contractor/sub-contractor
Human Resources	• Present each new employee or contractor with the existing GPRC policies, upon the first day of commencing work with GPRC • Support all employees and students in the understanding of the requirements of this policy

All users (Employees and contractors, Students, Visitors and or Volunteers)	• Report all non-compliance instances with this policy (observed or suspected) to their Supervisor, Instructor or Institution Representative as soon as possible

8. Exceptions to the Policy

8.1 Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director.

8.2 Policy exceptions must describe:

8.2.1 The nature of the exception

8.2.2 A reasonable explanation for why the policy exception is required

8.2.3 Any risks created by the policy exception

8.2.4 Evidence of approval by the IT Director

9. Inquiries

9.1 Inquiries regarding this policy can be directed to the IT Director.

10. Amendments (Revision History)

10.1 Amendments to this policy will be published from time to time and circulated to the College community.

Appendix 1 - IT Security Incident Reaction Plans

1. Anti-malware Detection

Anti-malware tools may raise an alert when malicious code (i.e. adware, backdoor, dialer, downloader, exploit, hack tool, hijacker, key-logger, monitoring software, Remote Access Services (RAS), rootkit, spyware, Trojan, worm, etc.) has been detected. Note that anti-malware tools may also raise an alert for other threats such as malicious links found in emails, files or web sites.

ROLE	ACTIONS TO BE PERFORMED
Initial alert, confirmation of the incident, collection of information, and immediate response	
IT Help Desk	The first alert will typically be received as follows: a) A user reports an issue with a computer or device that presents a suspicious behaviour. b) A user reports an alert raised by the anti-malware installed on its computer. c) The central console of the anti-malware tool generates an alert. **Situation #1 - The malware detection is reported by a user, based on suspicious behaviour of a computer or device** – scenario (a) above: • Ask for and document all of the following information: o Date and time when the user reported the event o Name and phone number of the person that reported the malware o What is the type and name of the computer / device (Desktop/Laptop, Server, Smartphone, and/or Asset number) that presents a suspicious behaviour o The symptoms detected (suspicious behaviour of the machine) o Whether the user downloaded a file from the Internet, clicked on a link in an email, ran an executable file (.exe, .bat, etc.), or accessed suspicious web sites, before the first symptoms appeared • Through discussion with the user and the description of the symptoms, confirm if the suspicious activities are indeed suspicious (i.e. they are not a normal system behaviour or a symptom related to a new system install or update). Typical signs of a malware infection are: o Uncontrolled remote access (such as mouse moving by itself, windows and files opening or closing by themselves, etc.) outside of any authorized remote assistance or remote session o Files or system settings that have been modified or deleted, but not by the user o New applications or files installed o Any change in the computer screen (change of the background, new icons, or icons that disappeared, etc.) • If the suspicious behaviour is not confirmed send an email to inform the IT Support Manager and close the incident. • If the suspicious behaviour is confirmed, perform the following: o Ask the user to immediately disconnect the computer / server / device from the network, by disconnecting the network cable (for desktops, laptops and servers) and logically disabling all wireless connections (for laptops, smartphones and tablets), including Wi-Fi, Bluetooth, as well as GSM, 3G, H+ and LTE dongles.

ROLE	ACTIONS TO BE PERFORMED
	○ All decisions to disconnect production servers must be escalated immediately to the IT Systems Manager, who will decide if production servers can be disconnected. ○ Enquire with the user if the symptoms persist, once the physical and wireless networks have been disconnected. ○ Assign a ticket to the computer / device administrator to perform an advanced analysis of the machine. ○ Inform the IT Support Manager by email or phone call. **Situation #2 - The malware detection is reported by the anti-malware tool** (either through observation in the central console, reception of an email alert or alert reported by the user when the local anti-malware create a pop-up alert) – scenario (b) and (c) above: • Ask for and document all of the following information: ○ Date and time of the anti-malware alert ○ The type and name of the contaminated computer / device (Desktop/Laptop, Server and/or Asset#) ○ Name and phone number of the person that reported the malware (if applicable) ○ The name of the malware ○ The result of the automated clean-up (successful, quarantine, unable to quarantine) • If the result of the automated clean-up indicates that the malware has been successfully cleaned-up, deleted or quarantined, no specific action is to be taken and the incident can be closed. • If the result of the automated clean-up indicates that the malware could not be quarantined, perform the following: ○ Assign a ticket to the computer / device administrator to perform a manual removal of the malware and all related malware files ○ Inform the IT Support Manager by email or phone call
Support Technician Or Systems Administrator	• Verify that the computer / device has been disconnected from the network (i.e. physical disconnection of the network cable and logical disconnection from all wireless networks). • Review with the IT Support Manager or IT Systems Manager the decision to disconnect, based on the risk of malware propagation, data breach or any potential subsequent cyber risks as well as the impact to business and system operations and the need to maintain availability. • Take note of the malware name, time of detection, and result of the automated clean-up from the anti-malware console (or the local anti-malware logs). • If the malware could not be cleaned-up or quarantined, manually remove the malicious file, or follow the recommended instructions from the Anti-Malware vendor (This may include running a malware removal script).
Incident classification and escalation as required	
IT Managers	• When informed of the incident, review if any specific action is necessary beyond the required actions in this plan. Specifically, ensure that the impact assessment of the incident is complete and accurate and that sufficient remediation actions are identified to prevent any subsequent or unintended negative or adverse consequences to occur.

ROLE	ACTIONS TO BE PERFORMED
	• Decide if a production server should be disconnected.
Subsequent necessary actions	
IT Managers	• Decide if advanced investigation must be performed. Such investigation includes: o Taking an image of the computer before any test to preserve evidence. o Running a full scan of the machine using the installed anti-malware agent or a third-party anti-malware tool. If no malicious file is found, a second anti-malware engine may potentially be installed and run to confirm no threat is detected. If a suspicious file is found, review the vendor's recommended actions for clean-up. o Searching for evidence of a malware infection in registry files, ntuser.dat, system.dat and Sam files; system logs or new or modified services, users and/or startup events. If suspicious files are detected, make a copy of the infected file, file path info, and create a MD5 Hash to ensure integrity. • Use advanced tools (such as regripper, Mandiant "Red Line" and MFTdump) or obtain external security and forensics expertise.
Support Technician Or System Administrator	• Verify that suspicious activities are not occurring anymore and close the incident. • Fully reformat and re-install the computer, server or device before new release in production.

2. Loss of a Mobile Device (Laptop, Tablet or Smartphone)

GPRC does not authorize the use of personally-owned devices to connect to GPRC networks or process GPRC data. This plan applies to GPRC owned devices; however, if a user reports a loss or theft of a personally-owned device, IT Help Desk must enquire if this device was in any way used to process or store GPRC sensitive information (by transferring files through a USB physical connection for example) to assess the risks of a confidential or personal data breach.

Role	Actions to be performed
Initial alert, confirmation of the incident, collection of information, and immediate response	
IT Help Desk	The first report will potentially be received as follows: a) A user reports having lost a device. b) An individual (who is not the user of the device) reports having found a GPRC device. **Situation #1 – A user reports a lost or stolen device** – scenario (a) above: • Ask for and document all of the following information: o Date and time when the user reported the event o Name and phone number of the person that reported the event o Date, time and location when the device was viewed for the last time o Date and time when the device was considered lost or stolen o Brand, type name and asset number of the device o Indication if the device contains any confidential, sensitive or Personally Identifiable Information (PII) documentation / data / information – this includes students' data, confidential emails or files, financial information, strategic plans, HR files on personnel, etc. o Indication if any other items associated with the device have also been lost or stolen, such as external hard drives, DVD, USB keys or remote access token o Indication if any user names and password associated with the device have also been lost or stolen (such as a post-it note) • Confirm with the user if there has been an extensive search of the location where the device could have been left, or if there is evidence of a theft, such as "grab and run", forced doors or broken windows, and if any other items have also been stolen. • Immediately inform the IT Support Manager by email or phone call. • For mobile devices managed with an MDM (Mobile Device Management) tool, perform the following to remotely wipe the device: o Launch a request to wipe the device. If the request cannot be executed (if the device has been turned off, is not connected to the wireless network or if the GSM card has been removed), launch the wipe request multiple times at different times of the day or over a couple of days. o Report the result of the device wipe request to the IT Director. • Confirm with the user, the user's manager, as well as the IT Director, if an urgent replacement is necessary. • If a replacement is not required, the incident can be closed after the full circumstances of the loss have been documented. **Situation #2 – An individual other than the user reports a found device** – scenario (b) above: • Ask for and document all of the following information: o Date and time when the individual reported the event

Role	Actions to be performed
	○ Name and phone number of the individual that reported the event ○ Date, time and precise location of when and where the device was discovered ○ Brand, type name and vendor serial number of the device ○ Any identifiable information on the device, such as a person's name, an asset tag, a serial number, any specific marking, sticker or apparent marks or scratches ○ Indication if the individual tried to operate the device ○ Indication if any other item associated with the device has also been discovered (such as external hard drives, DVD, USB keys, paper documentation, binders, files, etc.). In this case, document each specific item and ask where exactly these items have been found (within the same device bag or piece of luggage for example) ○ Indication if any other authority or third party has been informed or involved after the device was discovered ○ Inquire why the individual contacted GPRC (i.e. what specific information led the individual to believe this is GPRC device) • Immediately inform the IT Director and the IT Asset Manager by email or phone call. Include as much of the above information as possible. • Assign a ticket to the IT Asset Manager.
Incident classification and escalation as required	
IT Managers	• When informed of the incident, review if any specific action is necessary beyond the required actions in this plan. Specifically, ensure that the impact assessment of the incident is complete and accurate and that sufficient remediation actions are identified to prevent any subsequent or unintended negative or adverse consequences to occur.
Subsequent necessary actions	
IT Assets Manager	• Investigate the loss of the device with the asset owner and its supervisor or manager. • Set-up and provide a new device as required. • Update the asset inventory.

3. Inappropriate Disclosure of Confidential or Personal Information

This procedure applies to any instance where confidential or personal data (as defined in the Record Classification and Handling Policy) has been potentially disclosed to unauthorized users. This type of event should be immediately reported whenever any suspicion of a risk of disclosure exists (i.e. the disclosure does not need to be formally confirmed before reporting).

Role	Actions to be performed
Initial alert, confirmation of the incident, collection of information, and immediate response	
Help Desk	The first report will potentially be received as follows, by any user: a) A sensitive paper document or electronic media is found left unattended (e.g. next to a printer, on a desk, etc.) b) A user has sent out an email with sensitive data to a wrong person, who is not authorized to see this information. c) Sensitive information has been posted on an Internet (or non-secure Intranet) web site or through social media. **Situation #1 – A sensitive document is found left unattended (e.g. next to a printer, on a desk, etc.)** – scenario (a) above: • Ask for and document all of the following information: o Date and time when the individual reports the event o Name and phone number of the individual that reported the event o Date, time and precise location when and where the document was discovered o Type of document (paper document, binder or report, CD, DVD, USB key, etc.). o Any identifiable information on the document, such as a person's name, a business team, a project name, or any specific marking. For an electronic document, ask if an asset tag or a serial number is on the media. o If the person reporting the event is not a GPRC employee or contractor, ask: ▪ Why the individual contacted GPRC ▪ If any other authority or third party has been informed or involved o Indication if any subsequent action has been performed such as contacting a business team or any specific data owner • Ask the user to bring the document (or media) to the Help Desk • If the document is an electronic document (CD, DVD, USB key, external media, etc.), clearly instruct the user not connect this media to any GPRC computer as it may potentially contain a malware. • Immediately inform The IT Director and the Privacy Officer (if personal data) by email of phone call. Include as much of the above information as possible. **Situation #2 – A user has sent out an email with sensitive data to a wrong unauthorized person** – scenario (b) above: • Ask for and document all of the following information: o Date and time when the event was reported o Name and phone number of the person that reported the event o Date, time when the email was sent out o Number of recipients of the email

Role	Actions to be performed
	o Name and contact information (phone) of the person that sent out the email o Name and contact information (phone) of the recipient(s) of the email o Indication of the type of confidential data in the email: ▪ Content (personal, financial, etc.) ▪ Format (Pdf file in attachment or text in the body of the email) ▪ Volume (number of attachment, unique data, pages, etc.) o Ask the user to forward a copy of the email to the Help Desk if possible o Indication if any subsequent action has been performed such as contacting the recipient (second email or phone call) or using the "recall" function of Outlook • Immediately inform the IT Director and the Privacy Officer (if personal data) by email or phone call. • Assign a ticket to the email server support group to clean-up, where possible, any location where this email has been wrongly disclosed, including: o Mail box of any internal unauthorized user o Public facing SMTP relay(s) o Internet based mailboxes, if applicable **Situation #3 – Sensitive information has been posted on an Internet (or non-secure Intranet) web site or through social media** – scenario (c) above: • Ask for and document all of the following information: o Date and time when the event was reported o Name and phone number of the person that reported the event o Date and time when the disclosure was observed o Name of the Internet site where the data was been discovered (web site, social media tool, etc.). o Exact URL text (web page link) of this location. Specifically, ask the user to send a copy of the link or a screenshot by email o Indication of the type of confidential data: ▪ Content (personal, financial, etc.) ▪ Format (Pdf file in attachment, text in the body of a web page, post in a blog, Twitter or any social media, etc.) ▪ Volume (number of attachment, unique data, pages, etc.) o Indication if any subsequent action has been performed such as contacting a business unit or any specific data owner • Immediately inform the IT Director and the Privacy Officer (if personal data) by email or phone call.
Incident classification and escalation as required	
IT Director and Privacy Officer (if personal data)	• When informed of the incident, review any evidence provided and inquire with Help Desk, the user that reported the incident or any other necessary stakeholder to assess the potential impact of the disclosure and if any specific action is necessary. Specifically, ensure that the impact assessment of the incident is complete and accurate and that sufficient remediation actions are identified to prevent any subsequent or unintended negative or adverse consequences to occur. • If the disclosure relates to an electronic document (a CD, DVD, USB key, external media, etc. or any media labeled "confidential"), never insert this

Role	Actions to be performed
	media in a computer connected to a network as it may potentially contain a malware. Instead, connect this media to an isolated test computer equipped with an anti-malware to verify the content of the media. • Instruct the system administrator to clean-up any location where this data has been wrongly disclosed (internal SharePoint sites, file shares, web servers, databases, etc.) where possible. • Review with senior management the need for: o A communication to the persons impacted by a privacy breach. o A report to the Office of the Privacy Commissioner. *Note the potential impact in terms of privacy breach disclosure:* • *Risk to personnel (students, employees, contractors, customers etc.): Identity theft; Financial loss; Threat to physical safety; Threat to emotional wellbeing; Loss of business or employment opportunities; Humiliation; damage to reputation or relationships; Workplace or social bullying or marginalization; etc.* • *Risks to GPRC: Litigation; Regulatory action; Possible liability; Statutory sanctions; Harm to reputation; etc.*
Subsequent necessary actions	
System Administrator	• Confirms if the clean-up operations (where applicable) have been successful and make a decision with the IT Director / the Privacy Officer (if personal data) to close the incident.
IT Director	• Take the opportunity to remind the user who caused the disclosure breach of what the required safe behavior is, as per GPRC IT and Security Policies, to prevent such disclosure. • If necessary, make a decision with the user's manager and Human resources to proceed with any disciplinary sanction.

4. Suspicious Network Traffic

Suspicious network traffic can be detected by either an IT administrator or any user.

Role	Actions to be performed
Initial alert, confirmation of the incident, collection of information, and immediate response	
Help Desk	The first report will potentially be received as follows: a) A user reports suspicious network activity. b) A network monitoring tool generates an alert. **Situation #1 – A user reports suspicious network activity** – scenario (a) above: • Ask for and document all of the following information: o Date and time when the individual reported the event o Name and phone number of the individual that reported the event o The type and name of the network, network device, network traffic and services, computer or device related to the suspicious activity o The symptoms detected o Indication if any user / application / system could have triggered the suspicious network traffic • Immediately inform the network administrator by email or phone call. Include as much of the above information as possible. **Situation #2 – A network monitoring tool generates an alert** – scenario (b) above: • Ask for and document all of the following information: o Date and time of the alert o The type and name of the network, network device, network traffic and services, computer or device related to the suspicious activity o If the alert relates to a potential intrusion (i.e. alert generated by an IPS/IDS): ▪ What are the technical details related to the intrusion: IP address origin and destination, port number used, services used, any other useful information ▪ What is the time period during which the intrusion was detected and what is the volume of alerts received o If the alert is related to a peak of network traffic: ▪ What is the normal traffic load vs. the observed load ▪ What is the time period during which this peak was observed • Immediately inform the network administrator by email or phone call. Include as much of the above information as possible.
Network Administrator	**Situation #1 – A user reports suspicious network activity** – scenario (a) above: • Based on the information communicated, confirm if the suspicious activity is indeed suspicious (i.e. not a normal system behaviour or a symptom related to a new application / server / service / firewall rule change, install or update). Contact the user that detected the symptoms for more information. Typical signs of a malicious intrusion or malware are: o Use of an unusual port number o Unusual volume of traffic o Source IP address corresponds to either:

Role	Actions to be performed
	▪ A non-Canadian country, or a location that does not participate in any business with GPRC o A user that is not normally authorized to access the targeted resource o Destination IP address corresponds to a restricted network segment • If the suspicious network traffic is not confirmed, send a brief note (by email) to the IT Systems Manager and inform him of the incident. • If the suspicious behavior is confirmed, perform the following: o Escalate to the IT Systems Manager the decision to block the traffic, based on the risk of malware propagation, data breach or any potential subsequent cyber risks as well as the impact to operations and the need to maintain availability. *All decisions to block production network traffic must be approved by the IT* Systems Manager *to ensure no unnecessary disruption to production services is performed (i.e. the decision to block production network traffic must be risk based and should occur only if the intrusion is confirmed and the risk of further security breach is high).* o Verify with the user if the symptoms persist, once the network traffic has been blocked. **Situation #2 – A network monitoring tool generates an alert** – scenario (b) above: • Verify that the intrusion detection (IPS) tool has blocked the traffic automatically. • If the intrusion detection tool has not blocked the traffic automatically, escalate to the IT Systems Manager the decision to manually block the traffic, based on the risk of malware propagation, data breach or any potential subsequent cyber risks as well as the impact to business and system operations and the need to maintain availability • If the intrusion detection tool has blocked the traffic automatically, report to the IT Director and close the incident.
Incident classification and escalation as required	
IT Systems Manager	• When informed of the incident, review if any specific action is necessary beyond the required actions in this plan. Specifically, ensure that the impact assessment of the incident is complete and accurate and that sufficient remediation actions are identified to prevent any subsequent or unintended negative or adverse consequences to occur.
Subsequent necessary actions	
Network Administrator	• Initiate an investigation where necessary, by gathering logs of the network, firewall, and systems related to the suspicious traffic, as well as any other necessary evidence for further analysis, as required. • Make a decision with the IT Director to keep the new network restrictions, or to restore the normal network traffic, and close the incident.

5. Suspicious User Activity

Suspicious user activity will generally be detected by another user, through direct or indirect observation of a user's behaviour violating GPRC IT and Security Policies.

Role	Actions to be performed
Initial alert, confirmation of the incident, collection of information, and immediate response	
Help Desk	A suspicious user activity can be detected by another user or cyber security tools, such as Anti-Malware, Email or Web Content Filtering, as well as Data Loss Prevention (where applicable) could also send an alert. • Ask for and document all of the following information: o Date and time when the user reported the event. o Name and phone number of the user that reported the event o Description of the suspicious user activity o Estimated level of risk induced by this activity and information supporting this assessment. • Immediately inform the IT Director or Physical Security (where applicable) by email or phone call. Include as much of the above information as possible.
Incident classification and escalation as required	
IT Director	• When informed of the incident, immediately review the details of the suspected activity and make a decision if an immediate threat is possible. For example, the IT Help Desk should disconnect a user or deactivate a user account, if a user is downloading illegal content or is uploading confidential data outside of GPRC internal networks • Immediately inform the necessary system administrator or Physical Security (where applicable) by email of phone call. *Note that all information related to a user's suspected behavior must be carefully protected as confidential. It is critical that all personnel aware of such suspected behavior do not publicly communicate this information, or communicate it to anybody not already aware of these facts (with the exception of the IT Help Desk, Human Resources (HR) or the IT Director). This includes the user, the user's supervisor or manager, the user's colleagues, etc., unless specifically required as part of the investigation.* *Note that the decision to directly contact the user assumed to be involved in the suspicious activity must be carefully considered. It is critical that this decision be made by the IT Director, the user's manager (where applicable) and HR. A decision not to immediately contact this user can be made when it is either necessary to:* o *Gather sufficient evidence before taking action.* o *Confirm that the reported suspicious activity is real, to prevent any false accusations.* • Specifically, ensure that the impact assessment of the incident is complete and accurate and that sufficient remediation actions are identified to prevent any subsequent or unintended negative or adverse consequences to occur.

Role	Actions to be performed
Subsequent necessary actions	
IT Director and Physical Security (if applicable)	• Where applicable, take the opportunity to remind the user who caused the suspicious activity of what the required safe behavior is as per the GRPRC IT and Security Policies. • If necessary, make a decision with the user's manager and Human Resources to proceed with any disciplinary sanction, engage authorities (police, justice, etc.), perform a forensics investigation, etc.

6. Web site Defacement

This plan relates to all gprc.ab.ca websites. Note that GPRC may also manage other web sites, including https://www.facebook.com/pages/Grande-Prairie-Regional-College-GPRC/441390429205593. For GPRC Facebook and Twitter websites, as well as any other websites, this reaction plan may also be used although it may not cover important areas or may not involve the same persons.

Role	Actions to be performed
Initial alert, confirmation of the incident, collection of information, and immediate response	
IT Help Desk	The report will potentially be received as follows: a) A user reports errors on the GPRC website. b) The GPRC website administrator reports that the web site has been defaced, i.e. unauthorized changes have been made to the website. **Situation #1 – A user reports errors or changes to the website** – scenario (a) above: • Ask for and document all of the following information: o Date and time when the user reported the event. o Name and phone number of the user that reported the event o Description of the website errors or changes o The URL of the specific page(s) that present(s) errors or has/have been changed. o Ask for the user's web browser name (Chrome, Internet Explorer, Mozilla, Safari, Opera, Dolphin, etc.) and version. Instruct the user to open the following link to confirm the browser name and version: http://whatbrowser.org/. • Open the documented URL on your local computer to visually confirm the web page(s) errors or changes reported by the user (i.e. these errors or changes are not related to the user's browser or computer environment) and take a screenshot. If the errors or changes reported cannot be visually confirmed, ask the user to send a screenshot by email. • If the reported errors or changes are confirmed and include symptoms of a hacker's defacement of the site, immediately inform the IT Director and the web site administrator by email or phone call. Include as much of the above information as possible in the ticket or any further communication. Example of a hacker's defacement of the site includes text such as "Hacked by < name or logo>", "H4ck3d", "Own3d", "Defaced", "D3f4c3d", display of any vulgar or vindictive language, pop-up windows, text or animations that cover the text normally displayed on the website. • If the reported errors or changes are confirmed but do not include signs of a hacker's defacement of the site, assign a ticket to the web site administrator to

Role	Actions to be performed
	perform a review of the website. Include as much of the above information as possible, as well as a copy of the screenshot (if applicable), in the ticket. • If the reported errors or changes are not confirmed, send a note by email to the web site administrator for further investigation. **Situation #2 – Unauthorized changes to the website are reported** – scenario (b) above: • Ask for and document all of the following information: o Date and time when the site administrator reported the event o Name and phone number of the administrator that reported the event o Description of the website errors or changes, including: ▪ The URL of the specific page(s) that present(s) errors or has/have been changed ▪ The specific text being displayed o Indication if these errors or changes appear to all users accessing the web site whatever their location (Canada, US, Rest of the world) or the browsers they use • Open the documented URL on your local computer to visually confirm the web page(s) errors or changes reported by the site administrator, and take a screenshot. • If the reported errors or changes include symptoms of a hacker's site defacement, immediately inform the IT Director by email or phone call. Include as much of the above information as possible in the ticket or any further communication. Example of hacker's site defacement includes text such as "Hacked by < name or logo>", "H4ck3d", "Own3d", "Defaced", "D3f4c3d", display of any vulgar or vindictive language, pop-up windows, text or animations that cover the text normally displayed on the website. • If the reported error or change does not present any sign of a hacker's site defacement, assign a ticket to the web site administrator to investigate (for traceability). Include as much of the above information as possible in the ticket.
Web Content Manager	• If it's not possible to fix a defacement within an hour, (i.e. to restore the normal functionality of the website, such as the normal web page or content to be displayed), a decision to disconnect the web site from the Internet must be made with the IT Director as well as the Communication Officer, based on the risk of any further data breach or security risks, as well as the impact to business operations, communications and the need to maintain the availability of any function of the website.
Incident classification and escalation as required	
IT Director	• When informed of the incident, ensure that the impact assessment of the incident is complete and accurate and that sufficient remediation actions are identified to prevent any subsequent or unintended negative or adverse consequences to occur. *Note that a web site defacement potentially incurs the following risks:* o *Impact to GPRC image, when the defacement is publicized.* o *Impact to GPRC operations, when the web site is used by GPRC stakeholders for specific communication needs or business processes.*
Subsequent necessary actions	

Role	Actions to be performed
Web Developer / Web Content Manager	• If necessary, and as part of the cyber security incident process, change user login credentials of any users that have administrator access to the web site and to all the CRM tools used to manage the content of the web site, before restoring the web site. • Perform a restoration of the latest safe instance of the web site.