Functional Impact Guide

Courtesy of

Nebraska Cybersecurity Network for Education

Adapted from CDW

February 2025

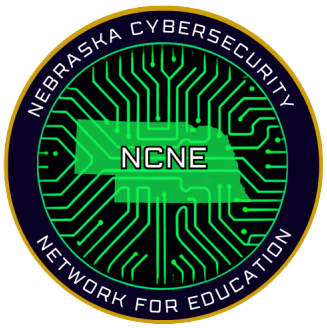

Table of Contents

Introduction

In the Incident Response Plan Template, there is a definition of Functional Impact Levels that are to be used when classifying an incident. Functional Impact will be evaluated to determine the business impact on availability of data, systems, end users, and business operations. The following table serves as a reference to applicable functional impact levels to be evaluated when determining overall incident severity.

Functional Impact Determination			
Select functional severity based on Functional Impact			
Symbol	**Functional Impact**	**Description**	**Recommended Severity**
H	High	Cannot provide a critical service to any user	HIGH/Level 3
M	Medium	Lost ability to provide an essential or deferred service. Reduced ability to provide a critical service	MEDIUM/Level 2
L	Low	Minimal effect: can still provide all critical, essential, or deferred services to most users, but has lost efficiency	LOW/Level 1
N	None/No	No effect in ability to provide all services to all users	LOW/Routine

In order to better understand that one incident type may yield a functional impact in more than one of these levels, this document attempts to provide a list of attack and incident types, then provides examples for each attack and incident type on how variations of each attack and incident may result in a different functional impact level. As this document is a guide, is it designed as a general reference.

Disclaimer

The general list of attack and incident types is not meant to be exhaustive and include every possible type of attack or incident. The school or ESU should carefully review each type and decide if there are relevant and potential attack or incident types that are not included and to include them.

Additionally, the examples of attacks or incidents that are presented at each functional level are meant to be general examples and may not be relevant to all environments. It is the responsibility of the school or ESU to review each example carefully to decide if they agree with the level of the example based on their unique environment.

Once all attack and incident types have been reviewed and updated, as necessary, and once all the examples provided have been reviewed and updated, as appropriate, this document may be referenced to help consistently identify the correct functional impact level for any incident that is encountered.

General List of Attack and Incident Types

- **Ransomware Attacks** – Cybercriminals encrypt school data and demand payment for decryption, often targeting districts with limited IT resources.
- **Phishing & Social Engineering** – Attackers trick staff, students, or administrators into revealing sensitive information through fake emails, messages, or phone calls.
- **Data Breaches** – Unauthorized access to student, staff, or financial records due to weak security controls or insider threats.
- **Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks** – Overloading school networks with excessive traffic to disrupt online learning, testing platforms, or administrative systems.
- **Malware & Spyware Infections** – Malicious software that compromises systems, steals data, or disrupts operations.
- **Unauthorized Access & Insider Threats** – Employees, students, or attackers gaining unauthorized access to systems, either maliciously or accidentally.
- **Third-Party Vendor & Supply Chain Attacks** – Cyber threats that exploit vulnerabilities in school technology providers, software, or services.
- **Internet of Things (IoT) Vulnerabilities** – Security weaknesses in smartboards, security cameras, or other connected devices used in classrooms.
- **Online Harassment & Cyberbullying** – Threats, harassment, or abuse occurring through school networks or online platforms.
- **Fraud & Financial Scams** – Scams targeting school finances, such as fake invoices, payroll fraud, or donation scams.
- **Account Takeover (ATO) Attacks** – Attackers compromise student, teacher, or administrator accounts (often through phishing or credential stuffing) to gain unauthorized access to school systems.
- **Cloud Security Threats** – As schools increasingly use cloud-based learning and administrative platforms, misconfigured settings, weak authentication, or compromised credentials can expose sensitive data.
- **Zero-Day Exploits** – Attackers take advantage of unpatched or unknown software vulnerabilities, potentially compromising school networks before a fix is available.
- **Physical Security Breaches Leading to Cyber Incidents** – Unauthorized access to school facilities where computers, network devices, or servers are left unsecured can lead to data theft or sabotage.

- **Misuse of AI and Generative Technology by Students** – Students using AI tools to manipulate grades, bypass security controls, or generate harmful content could introduce new security and ethical concerns.
- **Unsecured Personal Devices (BYOD Risks)** – Students and staff using personal, unprotected devices on school networks can introduce malware, data leaks, or unauthorized access points.
- **Third-Party App & Browser Extension Risks** – Unapproved educational apps, extensions, or plugins can introduce vulnerabilities or data privacy concerns when used in a school environment.
- **Electronic Resource Manipulation** – Unauthorized changes to online gradebooks, attendance records, or student information systems that impact academic integrity and operational reliability.
- **Network intrusions -** Unauthorized individuals may attempt to gain access to a school's network infrastructure for malicious purposes, potentially leading to data breaches, system disruptions, or espionage.
- **Malvertising**: The practice of using online advertising to spread malware.

Examples of Incidents

Ransomware Attacks Functional Impact Examples:

- **High Functional Impact**: A ransomware attack that encrypts all school data, including student grades, attendance records, and personal information. As a result, the school district is unable to provide any critical services related to student data access or management, affecting all users (students, teachers, administrators).
- **Medium Functional Impact**: A ransomware attack that encrypts important school documents such as lesson plans, report cards, and financial records. Although the district can still provide some essential services (e.g., in-person instruction), it cannot access critical data necessary for effective teaching and administrative functions. The reduced ability to provide a critical service causes disruption and frustration for students, teachers, and staff.
- **Low Functional Impact**: A ransomware attack that encrypts non-essential school documents like old meeting minutes or outdated reports. Although the district experiences some loss of efficiency due to the time spent on recovering or rebuilding these files, it can still provide all critical, essential, or deferred services to most users with minimal impact on their daily activities.
- **No Functional Impact**: A ransomware attack that targets an outdated server containing only obsolete data. The school district does not lose access to any critical, essential, or deferred services for students, teachers, or administrators and can continue operating without any disruption.

Phishing & Social Engineering Incidents Functional Impact Examples:

- **High Functional Impact**: A phishing attack successfully gains access to the school district's network by tricking an administrator into revealing their login credentials for the student information system. This results in a complete loss of access for all users, affecting critical services such as enrollment, attendance tracking, and report cards, causing significant disruptions to daily operations.
- **Medium Functional Impact**: A phishing email is sent to teachers and staff members, asking them to click on a malicious link to reset their school email passwords. Several employees fall for the scam and reveal their current passwords, leading to compromised accounts and unauthorized access to sensitive information. Although critical services are still available, the incident causes delays in communication and potential data breaches.
- **Low Functional Impact**: A student receives a phishing email pretending to be from a popular online gaming service, asking for their login details. The student clicks on the link but does not provide sensitive information since they are aware of the risk of

phishing attempts. Although the incident affects one user and potentially reduces their efficiency, all critical services remain available.

- **No Functional Impact**: A phishing email is sent to students requesting their personal information, but it is easily identified as a scam due to poor grammar and formatting. No users fall for the scam, and no sensitive information is compromised. All services continue functioning as usual without any impact on the school district's operations or end-users.

Data Breaches Incident Functional Impact Examples:

- **High Functional Impact:** A school district experiences an extensive data breach where unauthorized individuals gain access to sensitive student and staff information, including social security numbers, addresses, and educational records. The district's database server is compromised, leaving the entire system incapable of providing any services related to student or staff data until it is fully secured and restored.
- **Medium Functional Impact:** A hacker gains unauthorized access to a school district's financial records database, exposing confidential information such as bank accounts, tax documents, and vendor contracts. While the breach does not affect student or staff data directly, the district loses its ability to process financial transactions for several days until the issue is resolved, causing disruptions in payroll, purchasing, and other financial operations.
- **Low Functional Impact**: A school district experiences a data breach where an unauthorized individual gains access to student grades and attendance records. The district's IT team identifies and patches the security vulnerability that allowed the breach but continues to experience reduced efficiency in managing student data until the system is fully restored and all affected records are reviewed for accuracy.
- **No Functional Impact**: A school district detects a potential data breach attempt where an unauthorized individual tried to gain access to sensitive student and staff information. However, the district's strong security controls quickly identify and block the intrusion, preventing any unauthorized access or data theft. The incident has no effect on the district's ability to provide all services to its users.

Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attack Functional Level Examples:

- **High Functional Impact**: A large-scale DDoS attack targets the school district's main network, overwhelming it with excessive traffic. As a result, all online learning platforms, testing systems, and administrative systems are unavailable to students, teachers, and staff. This makes it impossible for anyone to access essential resources or submit assignments, causing significant disruptions to the educational process.

- **Medium Functional Impact**: A DoS attack targets the school's internet connection, disrupting online learning platforms, testing systems, and administrative systems for an extended period. Although some students are able to access offline materials and continue their work, the overall efficiency of the learning process is impacted due to the unavailability of digital resources. This forces teachers to adapt their lesson plans and causes delays in grading and submitting assignments.
- **Low Functional Impact**: A brief DDoS attack overloads the school's internet connection for a short duration, causing intermittent disruptions to online learning platforms, testing systems, and administrative systems. While most students are still able to access the necessary resources, the temporary outages lead to minor inconveniences and some loss of efficiency in completing assignments or participating in virtual classes.
- **No Functional Impact**: The school's network experiences a short-lived DDoS attack that is quickly mitigated by its security systems, ensuring minimal disruption to online learning platforms, testing systems, and administrative systems. Students are able to continue their work without any noticeable impact on the services they rely upon for education.

Malware & Spyware Infections Functional Level Examples:

- **High Functional Impact**: A schoolwide ransomware attack that encrypts all important data (student records, grades, teacher files) and disables essential systems such as the student information system, email, or the learning management system. This prevents teachers from accessing necessary materials and students from submitting assignments or accessing their grades.
- **Medium Functional Impact**: A targeted phishing attack on the school's administrative staff leads to the installation of spyware that steals login credentials and sensitive data, causing disruptions in the payroll system for several days until the issue is resolved and new login credentials are issued. Teachers can still access essential resources but are unable to receive their paychecks during this period.
- **Low Functional Impact**: A single teacher's computer becomes infected with malware due to a student clicking on a suspicious link in class. The teacher loses access to their files for a day while the IT department cleans and restores the system. The teacher can still teach the lesson using alternative resources, but has to spend extra time recovering lost data and reorganizing files.
- **No Functional Impact**: A student downloads a game that contains adware onto their personal device at school. The adware displays unwanted advertisements during class, but does not affect the school's network or critical systems. The IT department can easily remove the adware from the affected device with minimal disruption to the user.

Unauthorized Access & Insider Threats Functional Level Examples:

- **High Functional Impact**: A system administrator mistakenly grants unlimited access to a student's account, allowing them to access sensitive information (e.g., grades, personal data) of all students in the school district. This incident is considered high because it directly affects the privacy and security of many users and cannot provide a critical service (protection of confidential data).
- **Medium Functional Impact**: An attacker gains access to the school's grading system and changes grades for multiple students in one class, causing disruption to the academic process and delaying the progress of affected students. This incident is considered medium because it affects the essential service of maintaining accurate student records and the critical service of providing timely feedback on student performance.
- **Low Functional Impact**: A teacher accidentally shares a lesson plan with an unauthorized person through email, resulting in sensitive information being exposed to others. This incident is considered low because it has minimal effect on the school's ability to provide all critical, essential, or deferred services. Although there was an exposure of sensitive information, most users can still access their intended data and services.
- **No Functional Impact**: A student accidentally locks himself out of his online account but is able to quickly reset his password through the school's standard security protocol. This incident has no effect on the ability to provide all services to all users, as the student can still access their account after resetting their password.

Third-Party Vendor & Supply Chain Attack Functional Level Examples:

- **High Functional Impact**: A ransomware attack on the school's learning management system (LMS) provider, resulting in the unavailability of access to course materials, assignments, and grades for all students and teachers. This prevents any user from being able to provide a critical service, thus causing a high functional impact.
- **Medium Functional Impact**: A cyber attack on the school's meal management system, leading to intermittent outages in the ability to process payments for meals. While the system is still operational, its reduced availability affects the school's ability to provide an essential service (meals), making it a medium functional impact incident.
- **Low Functional Impact**: A breach of the school's online library system that temporarily disables book reservations but does not affect the overall accessibility of books or research materials. The system can still function, but its reduced efficiency in handling book reservations results in a low functional impact.

- **No Functional Impact**: An incident where there is no significant impact on the school's third-party technology services. For example, a minor software glitch in the school's grade tracking system that does not affect the overall functionality and availability of the service to users, resulting in no functional impact.

Internet of Things (IoT) Incident Functional Impact Examples:

- **High Functional Impact**: A widespread vulnerability is found in the smartboards used across the entire school district, rendering them inoperable for all users. This affects the educational process significantly as teachers rely on these tools for instruction and student engagement.
- **Medium Functional Impact**: A security camera system connected to the network experiences a breach, causing some cameras to malfunction or display incorrect footage. Although the educational process can still continue without these cameras, it may impact safety measures such as monitoring student behavior and managing emergency situations. Additionally, if the breach results in unauthorized access to sensitive areas like school offices or administrative buildings, this could also affect the district's ability to provide essential services like communication with parents and staff.
- **Low Functional Impact**: A smartboard in one classroom is compromised by a known vulnerability, but the school has a backup device that can be used temporarily while the affected board is being repaired or updated. The educational process is not significantly disrupted due to this isolated incident, but it still causes minor inconvenience for the teacher and students in that specific classroom.
- **No Functional Impact**: A single security camera connected to the network experiences a temporary glitch, causing it to stop working temporarily. However, the school's overall ability to provide all services to all users remains unimpacted as there are multiple cameras covering different areas throughout the school and additional security measures in place. Once the issue with the affected camera is resolved, normal operations can continue without any disruption or loss of efficiency.

Online Harassment & Cyberbullying Functional Impact Examples:

- **High Functional Impact**: A student is repeatedly threatened and bullied on a school's online platform by multiple students to an extent that it creates a hostile environment for the victim. The school network's inability to prevent this behavior causes disruption in the educational process, affecting all users (students) who are using the network for learning purposes. This incident significantly impacts the school's ability to provide a critical service - ensuring a safe and conducive learning environment.
- **Medium Functional Impact**: A teacher is subjected to harassment on a school's online platform by a parent, causing discomfort and distraction. Although the school network

can still function, the incident affects the teacher's ability to focus on teaching duties, impacting the educational process for their students. The lost ability to provide an essential service (effective instruction) makes this incident medium in terms of functional impact.

- **Low Functional Impact**: A student posts inappropriate content on a school's online platform, which is viewed by other students but does not directly affect any critical services or disrupt the educational process. Although it causes some distraction and might lead to discussions that are not appropriate for a learning environment, the incident has minimal effect as most users can still access all essential services.
- **No Functional Impact**: A student shares personal photos with friends within a school-approved online collaboration platform designed for group projects. This behavior is not considered harassment or bullying and does not affect the availability of any data, systems, end-users, or business operations on the network. Therefore, there is no effect in the ability to provide all services to all users (students).

Fraud & Financial Scams Functional Impact Examples:

- **High Functional Impact**: A school discovers that a large amount of money was fraudulently transferred from their account due to a sophisticated payroll scam. The incident affects all staff members' salaries, resulting in an immediate halt of essential services like hiring new teachers and purchasing necessary supplies.
- **Medium Functional Impact**: School administrators receive multiple fake invoices for expensive items or services that the school did not order. Although these expenses are avoidable, they can impact the school's budget and force them to delay or cancel planned purchases of essential materials.
- **Low Functional Impact**: A donation scam email is sent out to parents, students, and staff from an account masquerading as the school's official email address. The scam asks for contributions to a nonexistent school project. Although some donations are lost, the school can still continue its operations as the financial loss is minimal compared to their overall budget.
- **No Functional Impact**: School officials become aware of a phishing attempt targeting their financial information but quickly identify and block it before any sensitive data is compromised or funds are transferred. In this case, there is no impact on the school's ability to provide services to users as they were able to prevent the incident from causing harm.

Account Takeover Incident Functional Impact Examples:

- **High Functional Impact**: An attacker compromises the account of a school principal and gains access to the administrative system, preventing the principal from performing their critical duties such as scheduling, grading, and communicating with staff and parents. This incident would significantly impact the school's operations, causing a high level of disruption.
- **Medium Functional Impact**: A teacher's account is taken over during online class sessions, disrupting the live lessons and preventing students from receiving instruction. Although alternative teaching methods can be employed to continue delivering essential content, the loss of real-time interaction with the class could negatively impact student engagement and learning outcomes.
- **Low Functional Impact**: A student account is compromised, but only affects their ability to access non-essential school resources like forums or extracurricular signups. The student can still complete their assignments and participate in classes, although with some inconvenience as they wait for the compromised account to be resolved.
- **No Functional Impact**: A teacher's account is compromised, but the attacker only changes the password and locks the teacher out. However, the school has a strong incident response plan that allows administrators to quickly reset the password and regain access to the account without any significant impact on teaching or learning. In this scenario, there would be no functional impact for users or the overall school operations.

Cloud Security Incident Functional Impact Examples:

- **High Functional Impact**: A school's cloud-based Learning Management System (LMS) storing sensitive student data is compromised due to misconfigured settings. The attacker gains access to all student records, including personal identifiable information (PII), and encrypts the data with ransomware, making it inaccessible to school administrators and teachers. As a result, the school cannot provide any critical service related to student data access or management, affecting all users.
- **Medium Functional Impact**: A teacher's account on the school's cloud-based email system is compromised due to weak authentication. The attacker gains unauthorized access to emails containing sensitive information about students and staff. Although the LMS is still accessible, the breach of confidentiality has significant implications for student privacy and data protection, reducing the ability to provide a critical service (data security).
- **Low Functional Impact**: A school's cloud-based calendar system has a configuration error that causes appointments and events to be delayed or missed. While the system is still functional, its effectiveness in scheduling and organization has been impacted, leading to reduced efficiency in managing school operations (minimal effect on ability to provide all essential or deferred services).

- **No Functional Impact**: A typo in a link shared for a cloud-based collaboration tool causes some users to be redirected to the wrong document. Users can still access and collaborate on the correct documents, and school operations remain unaffected as there is no loss of functionality or confidentiality in any system related to data, systems, end users, or business operations.

Zero-Day Exploits Incidents Functional Impact Examples:

- **High Functional Impact:** A zero-day exploit targeting the school's learning management system (LMS), rendering it completely inaccessible for all students and teachers during an important exam period, causing significant disruption to the educational process and critical services.
- **Medium Functional Impact:** A zero-day exploit compromises the school district's email system, making communication between staff members difficult and hindering essential services like student registration, parent-teacher communication, and vendor interactions. While some services might still be available, their effectiveness is reduced due to delays in response times and increased manual effort.
- **Low Functional Impact:** A zero-day exploit affecting the school's wireless network causes intermittent connectivity issues for students and staff throughout the day. Although all critical, essential, or deferred services can still be provided, the network instability results in decreased efficiency, as users experience slower response times and increased frustration while accessing online resources.
- **No Functional Impact:** A zero-day exploit targeting a rarely used school application has no effect on the ability to provide all services to all users. The affected application is isolated, and no critical or essential services are impacted, ensuring that the school's network remains secure and operational for its primary functions.

Physical Security Breaches Leading to Cyber Incidents Functional Impact Examples:

- **High Functional Impact**: An unauthorized individual gains access to the school's main office during non-business hours and steals multiple network servers containing sensitive student data, such as social security numbers, grades, and medical information. As a result, the school is unable to provide critical services like online grade reporting, student record access, or communication platforms that rely on the stolen servers, impacting all users (students, parents, teachers) significantly.
- **Medium Functional Impact**: A janitor discovers an unsecured computer in a classroom after hours and accidentally shuts it down while cleaning. The school's IT department is unable to restore the computer immediately due to a lack of spare parts, causing a delay in providing essential services like student learning applications or online testing

platforms. While some services may still be available, the reduced ability to provide critical services has an impact on students and teachers.

- **Low Functional Impact**: A network device is left unsecured during a school event, and an attendee gains unauthorized access. The intruder manages to download some outdated files containing non-critical information, such as old test papers or obsolete class rosters. Although the incident causes a minor disruption in efficiency, the school is still able to provide all critical, essential, or deferred services to most users.
- **No Functional Impact**: A visitor accidentally triggers the school's security alarm system during regular business hours while trying to find the main office. The IT department investigates and confirms that no computers, network devices, or servers have been compromised as a result of the false alarm. The school is able to provide all services to all users without any effect on their ability to access critical, essential, or deferred services.

Misuse of AI and Generative Technologies Functional Impact Examples:

- **High Functional Impact**: A student uses an AI tool to manipulate grades on a large scale, affecting the academic integrity of the entire school. This incident prevents the institution from providing a critical service (accurate grading) to any user (students and teachers).
- **Medium Functional Impact**: Multiple students collaborate and use an AI tool to bypass security controls, leading to unauthorized access to sensitive information such as grades, personal data, or exam questions. Although the system is still operational, the lost ability to maintain security and privacy of users' data constitutes a significant concern.
- **Low Functional Impact**: A few students use AI tools to generate harmful content, such as cyberbullying messages or inappropriate images, on school-issued devices or platforms. Although this incident disrupts the learning environment and may require additional resources to address, the school is still able to provide all critical, essential, or deferred services to most users, but has lost efficiency in maintaining a safe and positive learning environment.
- **No Functional Impact**: A student experiments with an AI tool to generate creative writing pieces for homework assignments without any negative impact on the system, data, end-users, or business operations. In this case, there is no effect in the ability to provide all services to all users.

Unsecured Personal Devices (BYOD) Incident Functional Impact Examples:

- **High Functional Impact**: A large number of students and staff members have connected their unprotected devices to the school network, allowing a malware infection to spread rapidly throughout the system. As a result, critical services such as email, student information systems, and online learning platforms are no longer accessible for any user.
- **Medium Functional Impact**: A group of students and staff have connected their unsecured devices to the school network, introducing malware that affects essential services like Wi-Fi connectivity or access to specific applications required for daily classroom activities. Although some critical services may still be available, they are significantly impacted, and the school cannot provide these services efficiently.
- **Low Functional Impact**: A few students and staff members have connected their unprotected devices to the school network, causing a data leak of sensitive information such as grades or personal student data. While all critical, essential, or deferred services are still available, the incident has resulted in a loss of efficiency due to the need for remediation efforts and potential notification requirements for affected individuals.
- **No Functional Impact**: A student attempts to connect an unsecured device to the school network but is promptly warned by security measures about the risks associated with using an unprotected device on the school's network. No data leak, malware infection, or unauthorized access occurs as a result. The school maintains its ability to provide all services to all users without any effect.

Third-Party App & Browser Extension Incident Functional Impact Examples:

- **High Functional Impact**: A school district has allowed unapproved educational apps that contain malware. The malware encrypts all the data stored on school servers, making it impossible for administrators and teachers to access essential educational resources, including student records, lesson plans, and grading systems. This incident severely impacts the entire district's ability to provide critical services to users.
- **Medium Functional Impact**: Students in a high school are using unapproved browser extensions for research purposes. These extensions have been found to collect sensitive data (e.g., search history, login credentials) without user consent, introducing potential data privacy concerns. Although the school can still provide essential services like access to the internet and educational materials, the breach of student data negatively affects their trust in the school's digital environment.
- **Low Functional Impact**: In a middle school, several students have installed unapproved educational apps that slow down the school-provided laptops due to excessive resource usage. Although the computers are still functional and can provide all critical services, their performance is significantly reduced, affecting the efficiency of both teachers and students during online lessons.

- **No Functional Impact**: At an elementary school, a few students have installed unapproved browser extensions that display advertisements while they are doing homework online. Although these ads might be distracting, the school can still provide all services to all users without significant disruption or data privacy concerns. The incident does not impact the critical, essential, or deferred services for most users in any meaningful way.

Electronic Resource Manipulation Functional Impact Examples:

- **High Functional Impact**: A system administrator unintentionally deletes an entire semester's worth of grade data for all students in a school district. This action causes a complete loss of critical service to teachers and students, making it impossible to access or submit grades, thus affecting the academic integrity and progress of all students.
- **Medium Functional Impact**: A teacher accidentally alters multiple students' grades in a subject, causing discrepancies in the records. While some essential services are still available (e.g., attendance data), the incorrect grade information affects the operational reliability and academic integrity for those particular students.
- **Low Functional Impact**: An unauthorized user changes a few student names or addresses in the school's database. Although it causes minimal disruption to the system, it may impact the efficiency of administrative tasks such as report generation, data analysis, and communication with parents. However, all critical services, including gradebooks, attendance records, and essential student information, remain accessible to users.
- **No Functional Impact**: A user makes minor typographical errors in names or addresses while updating a student's information through the system. These changes do not affect academic integrity, operational reliability, or availability of data, systems, end users, and business operations since they are easily corrected without causing any significant impact.

Network Intrusion Functional Impact Examples:

- **High Functional Impact**: A cyber-attack successfully penetrates the school district's main network, disabling access to all critical systems such as student information databases, email servers, and learning management platforms for all users. This prevents any user from accessing necessary resources, rendering the school unable to provide a critical service to its students, teachers, and staff.
- **Medium Functional Impact**: An unauthorized individual gains access to the school's network, disrupting internet connectivity in certain areas or affecting specific applications. While essential services like email communication and student information databases remain accessible, the reduced ability to provide a critical service—such as online

learning platforms or remote collaboration tools—results in limited functionality for some users.

- **Low Functional Impact**: An intruder manages to breach the school's network, causing a slowdown in performance across various systems like email servers and learning management platforms. Although all critical, essential, or deferred services can still be provided to most users, the overall efficiency of these systems is compromised, leading to slower response times and potential inconvenience for end-users.
- **No Functional Impact**: A minor network intrusion occurs, but it doesn't affect the school's ability to provide all services to all users. For instance, a non-malicious probe of the network infrastructure might have taken place, or perhaps an unauthorized user was detected and removed without causing any service disruptions.

Malvertising Functional Impact Examples:

- **High Functional Impact**: A school district's website is heavily infected with malvertising, causing pop-ups and redirects that potentially expose users to harmful malware. As a result, the district's online learning platform becomes inaccessible for all students and teachers, preventing them from accessing critical educational resources and conducting remote lessons.
- **Medium Functional Impact**: A popular educational app used by students and teachers within a school district has been compromised with malvertising. This affects the app's functionality and user experience, causing frequent pop-ups and redirects that can potentially expose users to malware. While the app is still usable, its performance is significantly slowed down, impacting productivity and learning flow for students and teachers.
- **Low Functional Impact**: A school district's news or event website experiences a minor malvertising issue, causing occasional pop-ups that don't pose any immediate threat to users. Although the main functionality of the site remains intact, the frequent interruptions may cause some inconvenience for users while accessing non-critical information such as school updates or events.
- **No Functional Impact**: A student accidentally clicks on a malicious ad during online research, but the school's endpoint protection software detects and removes the potential threat without causing any disruption to the user's device or network infrastructure. The incident does not impact the availability of data, systems, end-users, or business operations for other users in the district.