hi-impact consultancy

hi-impact media

Hi-impact Schools' Security Policy

1. School Antivirus and Operating System Updates Policy

One of your first lines of defence should be preventing intrusions into your network. A solid anti-virus solution is absolutely critical and hi-impact have developed partnerships with preferred suppliers who we trust to protect your devices and data.

All school devices running Windows operating systems will be covered by adequate anti-virus protection. Should a school opt to supply their own anti-virus protection rather than hi-impact's recommended solution, hi-impact technical staff will state whether this product meets their definition of "adequate". In the event of a product being deemed inadequate, hi-impact technical staff will advise that they will ensure that all devices are covered, but that they do not accept responsibility for any breaches that occur as a result.

Apple Mac operating systems are currently not included in this policy as virus attacks are exceptionally rare on these devices. It is a school's responsibility to request any Apple Mac anti-virus protection.

Hi-impact does not recommend that staff use personal laptops on the school network. If school authorises such use they must inform hi-impact technical staff and ask for it to be checked for suitable anti-virus protection.

Guests and visitor access to the network should be controlled. Ideally, no unchecked laptops should be permitted onto the network (see wifi section in this document for more details). Should the school wish to authorise visitor devices, it will be the responsibility of the school for any infection that may occur as a result.

USB drives can be a source of virus infection. Please see the section in this document on portable drives including USB devices.

Incident	Responsibility	Notes
Breach from using non-recommended product	School	
Breach from device not having any protection installed	hi-impact	Provisos apply, including, but not limited to: Access to machines must have been possible at a mutually convenient time; A full and thorough handover from the previous technical support provider must have been completed where applicable; a reasonable amount of time must have been given (taking into account allocated and contracted support time) for a technician to have checked and installed protection.
Breach despite using recommended product	Anti-virus provider	
Breach due to out of date anti-virus definitions	hi-impact	Provisos apply, including, but not limited to: School are responsible for ensuring orders are placed; Access to machines must have been possible at a mutually convenient time; A full and thorough handover from the previous technical support provider must have been completed where applicable; a reasonable amount of time must have been given (taking into account allocated and contracted support time) for a technician to have checked and installed protection.

See appendix for the GDPR statement from Panda Security.

2. School Backup Policy

Prevention is a crucial first step, but security breaches do occur even with the most stringent protection in place. For these rare occasions, having a multi-layered backup policy in place is vital. Hi-impact's technical staff have spent many years working with various solutions and strategies and will recommend a series of onsite and offsite backup measures to give you as much chance as possible to recover data should loss, corruption or deletion occur.

See Disaster Recovery Plan later in this document for full details on this.

The recommended Backup Policy does NOT guarantee 100% protection against data loss - factors including, but not limited to, date and time of breach and severity of the attack can have an effect on the success of a restoration.

See the appendix for the GDPR statement from Redstor online backup.

3. School Password Policy

Password-related breaches can be caused by human carelessness, brute force attacks, systematic computerised hacks or simply neglect. There are numerous measures that can be put in place to minimise such risks and hi-impact have a set of recommended guidelines that your school should adhere to.

It is hi-impact's recommendation that all school staff are subject to the following password policy:

- Enforced password changes - 90 days
- Password complexity rules - Passwords must have at least six characters. Passwords can't contain the user title/role (eg head), name or parts of the user's full name, such as their first name. Passwords must use at least three of the four available character types: lowercase letters, uppercase letters, numbers and symbols.
- No reuse of old passwords
- Locking of accounts that do not meet the requirements
- Locking of accounts that attempt access with an incorrect password more than 3 times within a 5 minute period. Account will be locked until the administrator unlocks it.

Schools may opt to modify some of these policies and in this case it is entirely the school's responsibility in the event of a breach that occurs as a result. If the password policies are fully enforced, it is hi-impact's responsibility to ensure the policies are active and functioning. Password policies DO NOT guarantee 100% protection against a breach.

Hi-impact can not accept any responsibility for passwords that are written down or shared shared between staff / other individuals.

Hi-impact will enforce a password reset upon first login for a newly created account, or when password resets are requested by members of the school staff.

Where schools have their own in-house technicians who have access to servers and administrator accounts, it is the school's responsibility to ensure all sessions are logged out when not in use. Where possible, technicians should use remote console sessions rather than physically logging on to servers, also consider the physical location of your server - if in a room where other people can access, leaving sessions logged in obviously creates a greater risk of a breach.

4. School Data Security Policy

Data is valuable and in many cases extremely confidential and sensitive. Taking precautions to minimise the risk of losing data or allowing it to fall into the wrong hands is vital.

Measures put in place by hi-impact technical staff to protect against data loss can be undermined if data is not stored and transported in the recommended way.

- Mobile devices: All mobile devices that leave the school i.e. staff phones, staff iPads, should have a passcode set and should follow similar guidelines as passwords when it come sto sharing that information with others.

- Staff Laptops: Staff should not use their own laptops or personal computers to store school data with Personal Identifiable Information (PII). School data that is held on staff laptops should only be in the user's My Documents and is accessible outside of schools via Offline Files. The offline files cache should be encrypted using Bitlocker via Group Policy.

- Portable hard drives (including USB "pen drives") can be restricted in their use by server policies. However, it is the school's responsibility to request this. Hi-impact recommend that ONLY encrypted USB drives are used. If no policy to prevent the use of portable USB drives is enforced, it is the responsibility of the school to ensure that staff do not use unencrypted USB drives to store and transport data.

- Anti Virus: hi-impact recommends Panda Adaptive Defense 360. Virus definitions are updated automatically. The system should be set to 'Hardening' mode for no longer than two weeks, before being put into 'Locked' mode. This is the responsibility of hi-impact technicians.

- Windows Updates: AEM Autotask manages all the Windows Updates on the network. All critical patches are deployed automatically as soon as is possible. It is, however, the responsibility of the school to ensure that all computers are rebooted regularly to force updates to take effect (we recommend computers are fully rebooted at least daily)

- Lock Screen: An automatic lock screen policy should be set via Group Policy on all admin machines. An idle time of 5 minutes is recommended. This is not always practical for teaching staff, so it should be the responsibility of the teacher to manually lock their workstation when they are away from it, unless the school specifically requests that teaching staff computers are subject to the timeout policy.

- Remote Access is an alternative to moving data offsite with USB drives. Please see the section on Remote Access for more details.

5. School Internet Security Policy

Your choice of internet provider and the associated filtering of content and traffic is one of the biggest decisions you can make. This system is effectively the main route into and out of your school network for both intentional and unwanted data transfers. Hi-impact only works with providers who deal with schools. They understand the unique nature of school data security, the importance of firewalls and filtering and the impact a breach can have. Making sure you are aware of the various levels of provision is something hi-impact will assist you with.

hi-impact recommends Exa Networks as our preferred Internet provider for schools.

There are currently 3 types of web filter that Exa Networks supply to schools. School SLA forms contain options for selecting the desired level of filtering:

- SurfProtect: Websites bulk blocked by categories and individually via the URL. Google, Bing, and other HTTPS search engines not filtered via SurfProtect as they are encrypted sites and the filter cannot see this traffic. DNS forwarders ensure that the search engines own Safe Search is enforced and cannot be overridden.

- Fusion: A certificate is installed on all devices and in conjunction with a StormShield firewall which is situated internally, encrypted search engine traffic is filtered through the SurfProtect web filter.

- Quantum: Exa's newest filter. Similar to Fusion but without the need for the additional StormShield Firewall. Traffic is filtered on encrypted sites such as Google; it has a Keyword banned list; it is fully Active Directory integrated and can therefore track the users browsing history in compliance with the Prevent agenda.

All three solutions require the use of a Draytek firewall which monitors and controls incoming and outgoing network traffic based on predetermined security rules set by Exa Networks and hi-impact. Upon a breach being discovered, investigations by hi-impact and Exa Networks will be undertaken to determine the cause and the responsible party.

Whitelisting of websites can be requested by a school, to allow previously blocked websites to be permitted through the firewall. Hi-impact requires this request from the Headteacher, or designated other persons as specified by the Headteacher, and will make the requested change to the whitelist. Hi-impact technical staff may deem some requests as a potential risk, and will in such cases notify the school before making the change. It is not the responsibility of hi-impact to check every request though, and school staff must make their own background checks before making requests.

BYOD (Bring Your Own Device): This will be reviewed on a case-by-case basis and there is no standard policy to cover this.

Please see the Appendix for the GDPR statement from Exa Networks.

6. School Remote Access Policy

With schools looking to minimise the risk of staff losing or misplacing data on portable drives when offsite, remote access is increasingly important as it means staff can work on sensitive documents through without it ever physically leaving site. Of course, by its very nature, remote access does create a pathway into and out of your network, so it is extremely important that security measures are put in place to ensure that it is as protected as possible.

There are three ways that the school is open to Remote Desktop. Each is described below, with the measures taken to ensure as secure a means of access as possible.

- AEM Autotask: Remote Monitoring and Management solution that hi-impact uses to provide support to the school. It is only used by hi-impact technicians and is secured via a strong password policy with 2-step authentication.

- Access to the SIMS server: The default RDP Port is open for the SIMS team to access the SIMS server using standard Remote Desktop. They use a SIMS account with Administrator rights, which has a strong password. Access to the SIMS server is limited to members of the Administrators Group only. The RDP Port is only visible to the Public IP of the SIMS team and the hi-impact offices. The security of passwords in use for this purpose is the responsibility of the SIMS team and hi-impact will not store these.

- Access to Remote Desktop for Staff: There are virtual machines that run on servers within the school that staff can remote on to while offsite. Only members of the Remote Access group can gain entry. Members of this Group have been provided to hi-impact by the school, and a complex password enforced upon them. In addition,

there is software that runs on these machines that blocks a person's public IP address in the Firewall if they get their login details wrong three times. Such events are monitored and reported to hi-impact via an email alert through AEM Autotask.

- Breaches occurring as a result of user carelessness or password issues are the responsibility of the school.

- Configuration errors leading to a breach are the liability of hi-impact

Remote access is inherently a pathway into the school network and as such cannot be 100% guaranteed to protect against a breach. hi-impact's protection levels, when combined with a good password policy will ensure a secure means of access as possible.

7. School Email Policy

Many attacks on school networks occur due to simple email-born attacks. **Be very careful when opening attachments**, even if the message appears to be from someone you know. E-mail attachments infected with viruses are one of the most widely used methods for infecting PCs. Excellent advice on email best practice can be found here courtesy of University of Liverpool. https://www.liverpool.ac.uk/csd/email/effectiveuseofemail/

Educating your staff about common-sense measures to be concerned about when receiving and dealing with emails is obviously useful, but there are some steps you can take to further defend against email-related data loss.

hi-impact recommends the following security precautions:

- hi-impact recommends GMail as the preferred email solution.
- Staff should not use personal email accounts for school use.
- Email accounts should be secured using a strong password of at least six characters with three of the four available character types: lowercase letters, uppercase letters, numbers, and symbols.
- Email passwords should not contain parts of the user's full name, such as their first name. Neither should passwords contain elements of their role eg 'head' or 'office'
- Email password should not be shared or written down.
- Two step authentication should be enabled on all school email accounts, and enforced to require this process every time a user logs in.
- Google does not contain the function to auto logoff GSuite after a period of inactivity. Staff should be aware of this and sign out when not using the email system. Staff should be made familiar with the process of logging out of their email from another location. By simply scrolling to the bottom of the Inbox they can access *'Account Activity Details'* and then log out from all other signed in locations.
- Staff who use the GMail app on their mobile devices should have a passcode set to access that device.
- hi-impact holds the administrator login for the email system. The password meets complexity requirements.

- For emails that are Gmail to Gmail the traffic is encrypted. For emails that are from Gmail to another email provider, traffic is not encrypted. If the email contains sensitive data or PII then hi-impact recommends Virtru for point to point encryption.
- The misuse of the school email system is the responsibility of the school.
- An email retention policy is the responsibility of the school.

8. School Server Configuration Policy

Your server is not something you or your staff are likely to have any contact with. It is hi-impact's responsibility to make recommendations for the best and most secure setup and upon your instruction to implement these.

In some cases, schools may have their own in-house technical staff or request access to the server or an administrator account. If this is the case, the school will need to accept responsibility for any breaches that occur as a result. Ideally, your technical support provider should be the only party with this access as it reduces the risk by minimising the number of potential responsibilities.

The steps hi-impact recommend for configuring your server security are as follows:

Servers should be physically located in a lockable, secure room that cannot be accessed by non support staff, or inside a locked cabinet that prevents interference or theft.

Only members of the Administrators group can log in to the servers.

Groups and Security permissions: All school data is either held on the Domain Controller (staff and pupil files) or the SIMS server (SIMS and FMS databases). All data is secured by appropriate permissions and access is dependant on what security group the end user is a member of.

Group Policies: Some aspects of the security of the end users desktop experience is governed by group policies developed by hi-impact. They give a balanced mix of security and usability.

File Server Resource Manager (FSRM): To counter the threat of Ransomware attacks FSRM is running on the servers and prohibits changing of file extensions to a known list of threats. This list syncs daily with an ever increasing database of known ransomware extensions.

Windows Updates: AEM Autotask manages all the Windows Updates on the network. All critical patches are deployed automatically as soon as is possible.

See the Disaster Recovery Plan (12) for full details of this.

9.School WiFi Security Policy

Wireless networks are common place and indeed essential to the smooth functioning of a modern school. Mobile technology is prevalent both among staff and pupils and increasingly so, with visitors.

Wireless risks are usually confined to physical proximity to the school premises, which obviously helps contain the likelihood. However, encrypted password access is recommended for all wireless access points.

Hi-impact's recommended wireless network measures are as follows:

- hi-impact recommends Ubiquiti or Ruckus as the preferred Wireless solution.

- All wireless Access Points / Base Stations connected to the network should be registered and approved by hi-impact.

- All wireless access points that connect clients to the internal network (LAN) shall require users to provide unique authentication over secure channels and all data transmitted shall be encrypted with an approved encryption technology.

- A strong network key should be set. This network key should not be given out freely. The network key should not be written down and left in a visible place. School school need to change the WiFI password, it should be noted that this process is not as simple as many people perceive. Every device that connects wirelessly needs to be available for your technician and then reset. In larger settings this is a significant task and will invariably cause disruption to pupils and teachers as well as wasting valuable technical support time. For this reason we strongly recommend high levels of password security for your WiFi. Limiting the number of people who know the password will certainly decrease the risk of password related incidents.

- Visitor access to your network via wireless is often requested by schools. Visitor access should never be granted through your standard wireless network - a dedicated visitor strategy should be implemented in order to prevent access through the access points into your school network - it is only an internet connection that a visitor should require, and a visitor network can restrict usage in this way. Guest Wi-Fi should be set up and used for visitors. A token can be generated that allows access to the network for a certain period of time before it expires, and access is revoked. By default, hi-impact will NOT enable visitor access. If your school wishes to have a visitor access network configured, please let your technician know. *NB: Some wireless systems do not have the facility to allow visitor access, but your hi-impact technician will inform you if that is the case, following your request.*

10. Ex-Employees

School Staff: It is the responsibility of the school to inform hi-impact of any staff who leave or are dismissed, and hi-impact will implement the appropriate measures to ensure that accesses are revoked to the school network.

Hi-impact Staff: It is the responsibility of hi-impact to inform the school of any staff who leave or are dismissed, as well as revoking access from hi-impact systems and any remote facilities into the school. School should update their DBS lists for hi-impact to ensure that access to site cannot be granted for the ex-employee in question.

11. 3rd Party Providers

If changes are made to a school computer system or a new system is introduced without prior consultation with hi-impact which adversely affects system operation, hi-impact will not be liable for any faults that arise as a result. School will also need to cover any extra time taken to resolve such issues.

12. School IT Disaster Recovery Policy

Perhaps one of your most important considerations when it comes to security is knowing the processes for how you deal with a disaster. Minimising the impact of a breach and recovering data and operability could mean the difference between a few hours and a few weeks of downtime. Additionally, knowing that in the worst-case scenario your data can be fully or almost fully recovered provides peace of mind and enables the school to be back up and running as soon as possible.

This Disaster Recovery Plan has been developed by hi-impact consultancy as the optimum and recommended level of support that we can offer to a school. In order to ensure that this policy and the procedures within it are always relevant and current, a review will be carried out annually or following any significant changes to equipment or 3rd party providers.

Disasters are rare but when they do occur they can have devastating consequences. Many services will quickly be brought to a standstill in the event of a critical technical breakdown. As more reliance is placed upon digital systems, the threat of disaster is both more likely and more detrimental.

What is a Disaster?

In this policy a Disaster is defined as loss or damage of part or all of the school's ICT Infrastructure, which would have a high, or very high, business and educational impact upon the school.

This includes:

a) Total loss of one site, (i.e. due to fire damage)

b) Loss or technical failure of one or more network servers

c) Loss or technical failure of network infrastructure i.e. hub/switch/router/comms link

d) Major attack on the system by a virus or other type of malware.

The following policy highlights what systems a school should have in place and what systems are available to increase the security and safety of a school's data.

Admin Network:

- **Maintenance and Updates:**
  Servers and workstations are routinely checked for software and hardware faults. Antivirus definitions and Microsoft Updates are kept up to date.

- **Redundancy:**
  Server hard drives are configured with a minimum of RAID 1 redundancy, ideally RAID 5. This means the server can withstand a failed hard drive without any data loss.

- **Shadow Copies:**
  All data stored on the server is backed up twice a day (7:00 and 12:00) using a Microsoft system called Shadow Copies. All users are able to retrieve deleted work from anywhere on the network with a right click of the mouse.

- **Cloud Backup:**
  The Admin data and the SIMS server is backed up nightly using an offsite cloud backup solution. This means that all the schools Admin data is offsite and up to date. hi-impact use a system called Redstor (powered by Attix), which are one of the market leaders in this field and the only service to be authorised by Capita. All data is held within the UK, thus meeting with data protection requirements.

- **Internal Backup:**
  A full server backup is scheduled to run every night to an internal drive within the SIMS server. This is a *system image* backup, and is the quickest way to restore the server in the event of a catastrophic failure. Shadow Copies configured on this internal backup drive so 30 day's worth of backups are always available.

- **External Backup:**
  The file server is fully backed up to an external hard drive once every half term. This drive should be kept in a fireproof safe within the school, situated away from the server. This is in case of a site-wide disaster such as a flood or fire.

- **Power:**
  The server is powered through a UPS (Uninterruptible Power Supply) to prevent damage in the event of a power cut or power surge. In the event of a power cut, its function is to keep the server powered up long enough for it to shut down safely.

- **Email:**
  Email is cloud based and therefore accessible as long as there is an Internet Connection. In the event of prolonged loss of Internet Connectivity then an alternative connection could be established using a 3G device such as a phone or dongle.

Curriculum Network:

- **Maintenance and Updates:**
  Servers are routinely checked for software and hardware faults. Antivirus definitions and Microsoft Updates are kept up to date.

- **Mirrored Server:**
  The school has a second server, configured to replicate all the major roles with the primary server. This means that either server can go offline and the school will continue to function as normal.

- **Redundancy:**
  Server hard drives are configured with some redundancy, ideally RAID 5. This means the server can withstand a failed hard drive without any data loss.

- **Shadow Copies:**
  All the data that is stored on the server is backed up twice a day (7:00 and 12:00) using a Microsoft system called Shadow Copies. Any user is able to retrieve deleted work from anywhere on the network with a right click of the mouse.

- **Online Backups:**
  All User Areas and all Shared Areas are backed up nightly using Redstor (see above).

- **Internal Backups:**
  A full server backup is scheduled to run every night on to a dedicated drive within the SIMS server. This is a full system image backup, and is the quickest way to restore the server in the event of a catastrophic failure. The SIMS server is located away from the Curriculum server in another part of the building to reduce the risk of a fire damaging both servers. Shadow Copies is running on this internal backup drive so 30 day's worth of backups will be available.

- **External Backups:**
  The curriculum server is fully backed up to an external hard drive once every half term. This drive should be kept in a fireproof safe within the school, situated away from the server. This is in case of a site-wide disaster such as a flood or fire.

- **Power:**
  The server is powered through a UPS (Uninterruptible Power Supply) to prevent damage in the event of a power cut or power surge. In the event of a power cut, its function is to keep the server powered up long enough for it to shut down safely.

In the event of a Disaster:

- The Headteacher and hi-impact should be informed immediately.
- hi-impact will begin the disaster recovery process and inform school of realistic timescales.
- Where possible hi-impact technicians will attempt to repair any damaged equipment.
- Where possible hi-impact will loan any equipment required to speed up the recovery process.
- Should new equipment need to be purchased or external repair work carried out, school will receive a 'same day' quotation and order service.
- Throughout the process hi-impact will keep all key personnel fully informed of all progress.
- Should equipment be irreparable or any data found to be irrecoverable, hi-impact will not be held responsible or liable.
- Non School Days can be used for all Disaster Recovery work carried out by hi-impact technicians.
-

11. Policy Review

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant legislation.

Policy created: May 2018 Policy review date: May 2019

APPENDIX

Information and Policies from third parties with whom hi-impact and school directly engage:

- EXA: https://partners.exa.net.uk/pdf/education/information/exa-gdpr.pd
- REDSTOR: http://hi-impact.co.uk/wp-content/uploads/2018/03/REDSTOR-GDPR-DOC.pdf
- PANDA: http://hi-impact.co.uk/wp-content/uploads/2018/03/whitepaper-cybersecurity_compilance_EN.pdf
- GOOGLE: https://privacy.google.com/businesses/compliance/#?modal_active=none
- VIRTRU: https://www.virtru.com/gdpr-compliance/
- SQUARESPACE: https://static1.squarespace.com/static/5134cbefe4b0c6fb04df8065/t/58a4ae6de3df28f573c1c5fa/1487720821261/EEA+Data+Processing+Addendum.pdf

- AUTOTASK (CENTRASTAGE): http://www.autotask.com/gdpr-compliance