2024 NETWORK CONNECTION

Information and Communication Technology

Acceptable Use Policy

(AUP)

1. POLICY PURPOSE

The purpose of this Policy is to ensure the proper use of Information Communication and Technology (ICT) assets of the HERMANUS HIGH SCHOOL (HHS) NETWORK. The policy applies to any ICT asset the HHS Network has or may install in the future. Users have a responsibility to use ICT assets in an efficient, effective, ethical and lawful manner.

2. SCOPE OF APPLICATION

This Policy is applicable to all Western Cape Government (WCG) and School Governing Body (SGB) employees, school learners, contractor/agents who act on behalf of WCG or HHS or are in its employment and are end users of the WCG/HHS IT systems, equipment and infrastructure.

3. POLICY PRINCIPLES

The primary purpose of the Acceptable Use Policy is to protect the HHS Network school learners and contractors/agents who act on behalf of WCG or HHS or are in its employment, from illegal or damaging actions by individuals, whether deliberate or unintended. The primary guiding principle is that HHS Network Information Technology assets should ONLY be used for education purposes.

4. LEGAL FRAMEWORK

This Policy draws its mandate from the following prescripts:

- The Electronic Communications and Transactions Act (Act No. 25 of 2002)
- The Public Service Act (Act No. 111 of 1984)
- The National Strategic Intelligence Act (Act No. 39 of 1994)
- The Protection of Information Act (Act No. 84 of 1982)
- The National Archives and Record Service of South Africa Act (Act No. 43 of 1996)
- ABS/ISO 27k
- The Minimum Information Security Standards (MISS) and/or the Guidelines for the Handling of Classified Information (SP/2/8/1)
- The Regulation of Interception of Communications and Provision of Communication-related Information Act 2002 (Act No. 70 of 2002)
- South African Schools Act No 84 of 1996 with Amendments up to 2011

5. POLICY STATEMENT

5.1 General Provisions

5.1.1 The HHS Network is governed by a broad range of legislation regulating telecommunications including, but not limited to, the Electronic Communications and

Transactions Act of 2002, and the Regulation of Interception of Communications and Provision of Communication-related Information Act of 2002, (the Interception Act).

5.1.2 Users are bound by all relevant legislation and policies regulating telecommunications and electronic communications and undertake at all times to act in accordance with all relevant legislation and policies. Users acknowledge that they have been granted access by the organization to Telecommunications Information Technology and resources, including e-mail and Internet access. The sole reason for providing such access to users is to perform duties and responsibilities in accordance with their job function or other official purpose of the HHS Network.

5.1.3 Users acknowledge that they have no expectation of privacy when utilizing any telecommunications equipment and resources operated under the auspices of the HHS Network and they grant permission to the HHS Network to intercept, monitor, read, filter, block or otherwise act upon any electronic telecommunication, stored file or indirect communication which is or has been under their control, received by them or transmitted by them as contemplated in the RICA Act.

5.2 Use of School's Network IT Equipment

5.2.1 The learner shall be responsible for his/her workstation or portable device.

5.2.2 If the equipment is stolen, damaged, borrowed or otherwise unavailable for normal education activities it shall immediately be reported to the IT administrator or intern.

5.2.3 HHS Network equipment must not be removed from the School's Network premises without permission.

5.2.4 Every effort must be made to secure the equipment against theft.

5.2.5 Users must ensure that equipment assigned to them has received a unique identifier and is classified in accordance with the Asset Register.

5.2.6 Users with HHS Network equipment at their homes shall make every effort to safeguard the equipment as required by the *IT Security Policies*.

5.3 Desktop Computer Use

5.3.1 The device (Chromebook or Tablet) may not be connected to two or more networks simultaneously.

5.3.2 Users must be supplied with a username and password in order to access services on the school's network of the HHS Network.

5.3.3 Users must keep passwords secure and not share their account credentials. Users are responsible for the security of their own passwords and accounts.

5.3.4 The device must be kept up to date with the latest anti-virus software, virus definitions and Operating System updates.

5.3.5 The user must not disable, and/or change the configuration of the anti-virus software.

5.3.6 Users shall not load any illegal or unapproved software onto WCG equipment.

5.3.7 Users acknowledge sole responsibility for any unauthorized or pirated software found in their possession or on the systems and equipment allocated to or used by them.

5.4 e-MAIL

The HHS Network supports the installation and usage only of approved email clients. Usernames will be assigned by the HHS Network and reflect internally mandated e-mail naming conventions.

5.4.1 Acceptable e-Mail Use

5.4.1.1 Communicating in a professional manner.

5.4.1.2 Personal communications that are brief and do not interfere with school responsibilities.

5.4.1.3 Electronic messages are frequently inadequate in conveying mood and context. Users should carefully consider how the recipient might interpret a message before composing or sending it.

5.4.2 Unacceptable Use of Email

5.4.2.1 Creating and exchanging messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.

5.4.2.2 Creating and exchanging information that is in violation of copyright or any other law. The HHS Network is not responsible for use of e-mail that contravenes the law.

5.4.2.3 Opening file attachments from an untrustworthy source or with a suspicious or unexpected subject line.

5.4.2.4 Sending confidential information to unauthorized people or violating the Minimum Information Security Standards. Otherwise using e-mail in a way that increases the HHS Network's legal and regulatory liability.

5.4.2.5 Communications that strain the HHS Network or other systems unduly, such as sending large files to large distribution lists.

5.4.2.6 Circulating chain letters and/or commercial offerings.

5.4.2.7 Circulating unprotected data and personally identifiable client/citizen data that would violate section 14 of the Constitution.

5.4.2.8 Promoting or publishing a user's political or religious views, operating a business or for any undertaking that offers personal gain.

5.4.2.9 Using the e-mail system for any purpose or in any manner that may prejudice the rights or interests of the HHS Network.

5.5 Internet

Internet usage is granted for the sole purpose of supporting HHS Network activities. All Internet- based transactions originating from within the HHS Network are carefully monitored for auditing and compliance purposes.

5.5.1 Acceptable Uses of Internet:

5.5.1.1 Accessing web-based applications and tools.

5.5.1.2 Communication between Officials and non-Officials for business purposes.

5.5.1.3 Review of possible websites for educational purposes.

5.5.1.4 Reference regulatory or technical information in line with the relevant job description or official functions.

5.5.1.5 Accessing of Government websites and portals.

5.5.1.6 Conducting research in line with relevant job description or official functions.

5.5.2 Unacceptable Uses of Internet:

Acquisition, storage, and dissemination of data that are illegal, pornographic, or which negatively depict race, gender, sex, pregnancy, marital status, ethnic or social origin, sexual orientation, age, colour, disability, religion, conscience, belief, culture, language and birth, is specifically prohibited. The HHS Network also prohibits engaging in fraudulent activities, or knowingly disseminating defamatory materials.

Other activities that are strictly prohibited include, but are not limited to:

5.5.2.1 Accessing information that is not within the scope of the user's work. This includes unauthorized accessing and/or reading of HHS Network information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.

5.5.2.2 Deliberate pointing or hyper-linking of the HHS Network's websites to other Internet sites whose content may be inconsistent with or in violation of the aims or policies of the HHS Network.

5.5.2.3 Any conduct that would constitute or encourage a criminal offence, lead to civil liability, or otherwise violates any regulations, directives or the common law.

5.5.2.4 The use, transmission, duplication, or voluntary receipt of material that infringes on the copyright, trademarks, trade secrets, or patent rights of any person or organization. [Officials must accept that all materials on the Internet are copyrighted and/or patented unless specific notices expressly state otherwise].

5.5.2.5 Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls and the express permission from the relevant mandated parties.

5.5.2.6 Any form of on-line gambling and gaming.

5.5.2.7 Using the Internet for any purpose or in any manner that may prejudice the rights or interests of the HHS Network or WCG in any other sphere.

5.6 Information Security

5.6.1 All users accessing HHS Network information shall preserve the confidentiality, integrity and availability of information.

5.6.2 Users must ensure that all media, such as memory sticks, drives and CDs, that are to be discarded must be formatted and cleansed of all data, in such a manner that any repairing of the media and re-installing is made impossible.

5.6.3 Users must ensure that all media used for the storage of data is stored in a secure environment and within safe distance of any electro-magnetic interference, such as cell phones, that can damage the media.

5.6.4 Users must not share folders to all on the network from their computers without proper user logon authentication access security in place.

5.6.5 Users must not make any unauthorized copies of or modifications to the contents of any HHS Network information resources.

5.6.6 Users must handle all information resources in a secure manner.

5.6.7 Users must ensure that information under their control is backed up in line with the importance of the information to the HHS Network.

6. PRIVACY POLICY

6.1 The HHS Network maintains the right to monitor and review e-mail and Internet activity to ensure compliance with this Policy, as well as to fulfilling the HHS Network's responsibilities in terms of legislation. Users have no expectation of privacy.

6.2 On termination or separation from the HHS Network, access will be denied to e-mail and HHS Network Internet, including the ability to download, forward, print or retrieve any message stored in the system, regardless of sender or recipient.

6.3 Officials and learners who leave the HHS Network will have their mailbox disabled immediately after exiting the organization.

6.4 The HHS Network reserves the right to intercept, monitor, review and/or disclose any and all messages composed, sent or received. Intercepting, monitoring and reviewing of messages may be performed with the assistance of content filtering software, or by designated HHS Network Officials.

6.5 The HHS Network reserves the right to alter, re-route or block the delivery of e-mail messages as appropriate. This includes but is not limited to:

6.5.1 Rejecting, quarantining or removing attachments and/or malicious code from messages that may pose a threat to HHS Network resources.

6.5.2 Discarding attachments, such as music, that are considered to be of little value and involve a significant resource cost.

6.5.3 Rejecting or quarantining messages with suspicious content.

6.5.4 Rejecting or quarantining messages containing offensive language.

6.5.5 Re-routing messages with suspicious content to designated HHS Network employees for manual review.

6.5.6 Appending legal disclaimers to messages.

6.6 Electronic messages are permissible as evidence in a court of law.

6.7 Any content created with the e-mail system is considered the intellectual property of the HHS Network.

7. CYBERBULLYING

7.1 Cyberbullying is the process of using the Internet or mobile devices to send and post any text or images intended to hurt, torment, threaten, embarrass another person and includes any such conduct by way of email, mobile phone and text messages, instant messaging, personal websites and/or chat rooms.

7.2 Cyberbullying takes various forms including –

7.2.1 Instant Messaging (IM)/Text Messaging Harassment: sending hateful or threatening messages to the target/s.

7.2.2 Warning wars: reporting of provoked violations of Internet service providers' terms/website terms which can result in the target being banned from a particular website or social network.

7.2.3 Text wars or text attacks: ganging up on the target, including sending multiple text-messages to the victim's cell phone/ email.

7.2.4 Stealing passwords: masquerading as such a person and then posting inappropriate/ harmful/ illegal posts via such fake profile.

7.2.5 Sending/posting degrading pictures or videos.

7.2.6 Outing: sharing someone's secrets or embarrassing information online.

7.2.7 Trickery: tricking the target into revealing secrets or embarrassing information and then sharing it online.

7.2.8 Excluding: intentionally and maliciously excluding someone from an online or mobile device broadcast group.

7.2.9 Threatening the target with personal violence (including death threats) which may inspire fear or a belief in the victim that such personal violence is to take place.

7.2.10 Cyberstalking: reported and intense harassment, denigration and threats.

7.2.11 Internet Polling/Rating: Who's Hot? Who's Not? Who is the biggest nerd in the sixth grade? These types of questions run rampant on the Internet polls, all created by young people/ children.

7.2.12 Posting real or doctored images of the target.

7.2.13 Sharing personal or intimate information about the target.

7.2.14 Sharing contact information about the target coupled with a lewd solicitation ("for a good time call …" or "I am interested in [fill in the blank] …").

7.2.15 Sending porn and other junk e-mail and IMs: Often cyberbullies will sign their victims up for e-mailing and IM marketing lists, especially to porn sites, resulting in the victim receiving multiple e-mails from porn sites.

7.3 Role of WCG

7.3.1 WCG strives to create a climate in which every learner can develop academically, socially, spiritually and emotionally. In order for this to happen, Learners need to feel safe and supported, which includes WCG dealing with all elements of cyberbullying.

7.3.2 To further such principles, WCG has the right to deal with any incident of cyberbullying when it occurs via the ICT Systems or Personal Devices when linked to the Hermanus High School Wi-Fi.

7.3.3 WCG is entitled to deal with any incident of cyberbullying where:

7.3.3.1 cyberbullying takes place off campus or not via the ICT System where the cyberbully/ perpetrator is harming/ negatively affecting the target's education/ schooling or is disrupting learning in the classroom. For example: a learner cannot concentrate at school, is increasingly absent from school or results in fights at school/ in the classroom;

7.3.3.2 it impacts on the reputation or integrity of WCG/HHS; an employee, learner or parent;

7.3.3.3 a learner confides in a teacher/another learner about cyberbullying off campus or not via the ICT System and the teacher/other learner is concerned that such cyberbullying is harming the learner.

8. SOCIAL MEDIA

8.1 Social Media are the platforms that allow for interactive participation by users to create content and comment (one to one, one to many and many to many). Such communications can take place via any number of devices, such as computers, tablets, smartphones etc. Examples include Facebook, Twitter, Instagram, Whatsapp, Mxit, Google+, Tumblr etc.

8.2 Some examples:

8.2.1 Blogs - Short for “web-logs”, these are sites that can function as on-going journals with multiple entries. Online forums allow members to hold conversations by posting messages. Typically, entries are categorized with “tags” for easy searching. Most blogs allow for reader comments. Examples: Blogger, WordPress, Type Pad.

8.2.2 Micro-blogs - These blogs allow for shorter content posts, typically with a limited set of typed characters allowed. Micro-blogs can be used for status updates and to communicate information to “friends” or “followers” quickly. These are pushed out to anyone subscribed to receive the updates. Examples: Twitter, Tumblr.

8.2.3 Content communities / media sharing – services that allow you to upload and share various media, such as photos and videos. For example: YouTube, Flickr.

8.2.4 Bookmarking sites – services that allow you to save, organize and manage links to various websites and resources around the Internet. Example: Delicious, StumbleUpon, Pinterest.

8.3 Rules for Using Social Media as per the Social Media and Social Networking Policy

8.3.1 Access to Social Media is a privilege and not a right and is permitted at the sole discretion of WCG/HHS for learners over the age of 13.

8.3.2 WCG/HHS encourages the use of social networking/media (Twitter, Facebook, etc.) as a way to connect with others, share educational resources, create and curate educational content, and enhance the classroom experience. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private, personal or professional.

8.3.3 Use good judgment.

8.3.4 Regardless of privacy settings, assume that all of the information you have shared on your social network is public information.

8.3.5 Always treat others in a respectful, positive and considerate manner.

8.3.6 Be responsible and ethical.

8.3.7 Unless you are specifically authorized to represent WCG/HHS as a spokesperson, state that the views expressed in your postings, etc. are your own.

8.3.8 Do not publish, post or release information that is considered confidential or private. If it seems confidential, it probably is. Online “conversations” are never private.

8.3.9 Do not disclose your birth date, address, cell phone number on any public website.

8.3.10 To ensure your safety, be careful about the type and amount of personal information you provide. Avoid talking about personal schedules, situations, your school and places of after school activities.

8.3.11 NEVER give out or transmit personal information of learners, teachers, parents.

8.3.12 Do not post pictures/videos/information of any school activities without the consent of WCG/HHS.

8.3.13 Do not post pictures/videos/information of any learner, parent, teacher, visitor to the school without his/her express written consent.

8.3.14 When using social networking sites, comply with their terms and conditions.

8.3.15 Do not post defamatory or malicious comments about WCG/HHS, any learner, parent, teacher or other employee of WCG/HHS on any social media platform or via any mobile messaging application.

8.3.16 Do not use the WCG/HHS name or logos for endorsements.

8.3.17 Do not use the WCG/HHS logo or any school images or iconography on personal social media sites.

8.3.18. Do not use the WCG/HHS name or logo to promote any cause without prior consent.

9. PERSONAL DEVICES

The use of personal devices is NOT allowed for educational purposes.

9. STORAGE OF DOCUMENTS

10.1 Learners are provided with network locations in which to store documents and these locations are provided solely for storing school-related documents. These locations may not be utilized to store any personal information.

10.2 In particular, no personal photos, music and video clips may be stored on any part of the ICT System without the approval of WCG/HHS.

10. MONITORING

11.1 As part of the continuing effort to protect learners when using the ICT System and personal devices, and to ensure learners have a positive and safe experience, the user must acknowledge that WCG/HHS and its representatives may monitor, access, examine and intercept any communication on or via any component of the WCG ICT System or personal devices, by human or automated means. For such purpose, WCG has software that is designed to monitor each learner's use of the ICT System, all his/her communications and all usage of personal devices when connected to the WCG/HHS Wi-Fi.

11.2 Learners shall have no expectation of privacy when utilizing any component of the ICT System.

11.3 Learners shall co-operate with WCG/HHS to enable such access, and review, including providing any necessary passwords. Failure to co-operate with WCG in this way may result in disciplinary action being taken.

11.4 WCG may from time to time need to appoint external investigators and/or experts for the purposes of conducting forensic and other investigations into unlawful use and/or access to the ICT Systems and/or unlawful activities using the ICT Systems. Such external investigators and/or experts may need to access Learners' communications and/or the ICT System. No investigator/expert shall be granted access to any communications and/or ICT Systems, except for the sole purpose of conducting an audit/investigation as described/indicated in this clause.

12. DISCIPLINARY PROCESS

12.1 Breach of this policy may result in disciplinary action.

12.2 If you think you have breached the policy, please notify a teacher or the ICT support staff immediately so the school can take the proper steps to help minimize the impact it may have.

13. BREACH

Where a breach or a disregard of this policy has occurred, appropriate disciplinary action will be taken in line with the relevant HHS Network policies.

14. POLICY EFFECTIVE DATE

The policy will be effective on the date on which it is signed by the relevant authority.

15. APPENDIX – DIFINITION OF TERMS

Agents: A new type of software that performs special tasks on behalf of a user, such as searching multiple databases for designated information.

Confidential information: A designation for information, the disclosure of which is expected to damage the HHS Network or its business affiliates.

Critical information: Any information essential to the HHS Network business activities, the destruction, modification, or unavailability which would cause serious disruption to the HHS Network business.

Data Security Classification: The reference to "sensitive" data refers to the classification of the HHS Network data into two basic categories:

HHS Network Proprietary is information pertaining to business operations, new products, techniques, proposals or related information which, if compromised, would seriously impair the HHS Network operations.

HHS Network Private is information pertaining to business operations or individuals, and is of such importance to the HHS Network, or is so personal in nature, that indiscriminate release would have adverse effects on the HHS Network or the employee involved. Privileged employee information such as salaries and personnel records such as change requests is typical of the HHS Network Private.

Default password: An initial password issued when a new user-ID is issued, or an initial password provided by a computer vendor when hardware/software is first delivered.

Downloading: The transfer of data from a host computer (mainframe, minicomputer, network server, etc.) system to a connected workstation, such as a personal computer.

End-user: A user who employs computers to support business activities, who is acting as the source or destination of information flowing through a computer system.

Extended user authentication technique: Any of various processes used to bolster the user identification process achieved by user-IDs and fixed passwords (see hand-held tokens and dynamic passwords).

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed some security check (such as providing a password).

Information retention schedule: A formal listing of the types of information that must be retained for archival purposes and the timeframes that these types of information must be kept.

Log-in banner: The initial message presented to a user when he or she first makes connection with a computer.

Log-in script: A set of stored commands which can log a user into a computer automatically. Master copies of software: Copies of software which are retained in an archive and which are not used for normal business activities.

Password guessing attack: A computerised or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorised access.

Password reset: The assignment of another (temporary) password when a user forgets or loses his/her password.

Password-based access control: Software which relies on passwords as the primary mechanism to control system privileges.

Password: Any secret string of characters used to positively identify a computer user or process.

Positive identification: The process of definitively establishing the identity of a computer user.

Privilege: An authorised ability to perform a certain action on a computer, such as read a specific computer file.

Restricted Area: An area in which sensitive information is being processed or worked and therefore requires physical access controls.

Restricted information: Particularly sensitive information, the disclosure of which is expected to severely damage the HHS Network or its business affiliates (see confidential information).

Screen saver: A computer program that automatically blanks the screen of a computer monitor, CRT, LCD, Plasma after a certain period of no activity.

Security patch: A software program used to remedy a security or other problem (commonly applied to operating systems).

Sensitive information: Any information, the disclosure of which could damage the HHS Network or its business associates. Any data labelled as HHS Network secret or top secret.

Shared password: A password known by and/or used by more than one individual.

Special system privilege: Access system privileges allowing the involved user or process to perform activities which are not normally granted to other users.

Suspending a user-ID: The process of revoking the privileges associated with a user-ID.

Systems administrator: A designated individual who has special privileges on a multi-user computer system, and who looks after security and other administrative matters.

Uploading: The transfer of data from a connected device, such as a personal computer, to a host system (mainframe, minicomputer, server, etc.).

User-IDs: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Valuable information: Information of significant financial value to Parliament or another party.

Verify security status: The process by which controls are shown to be both properly installed and properly operating.

Virus: A parasitic software program, equipped with the means of reproducing itself, that spreads throughout a computer or network by attaching itself or infecting other software or diskettes. A worm is a similar program that propagates across a network by making copies of it.

Virus screening software: Commercially available software that searches for certain bit patterns or other evidence of computer virus infection.

2024 NETWERKKONNEKSIE

Inligting en Kommunikasietegnologie Aanvaarbare Gebruiksbeleid

(AUP)

1. BELEIDSDOELWIT

Die doel van hierdie beleid is om die behoorlike gebruik van die Inligtingskommunikasie- en Tegnologie (IT) bates van die HOËRSKOOL HERMANUS-NETWERK te verseker. Die Beleid is gerig op enige huidige IT-bate van die HHS-Netwerk of wat hierna bygevoeg mag word. Gebruikers het 'n verantwoordelikheid om sulke IT-bates bekwaam, doeltreffend, eties en wettig aan te wend.

2. TOEPASSINGSOMVANG

Die Beleid geld vir alle werknemers van die Weskaapregering (WKR) en Skoolbeheerliggaam (SBL), skoolleerders en kontrakteure/agente wat namens die WKR of HHS optree of in hul diens is en finalegebruikers van die WKR/HHS IT-stelsel, toerusting en infrastruktuur is.

3. BELEIDSBEGINSELS

Die hoofdoel van die Aanvaarbare Gebruiksbeleid is om die HHS-Netwerk, amptenare, skoolleerders, en kontrakteure/agente wat namens die WKR of HHS optree of in hul diens is van onwettige of skadelike handeling deur individue, hetsy doelbewus of onbedoeld, te beskerm. Die primêre rigsnoer is dat die HHS-Netwerk Inligtingstegnologiebates SLEGS vir onderrig(leer)-doeleindes aangewend word.

4. REGSRAAMWERK

Hierdie Beleid ontleen sy mandaat aan die volgende voorskrifte:

- Die Elektroniese Kommunikasie- en Transaksiewet (Wet 25 van 2002)
- Die Staatsdienswet (Wet 111 van 1984)
- Die Nasionale Strategiese Intelligensiewet (Wet 39 van 1994)
- Die Beskerming van Inligtingswet (Wet 84 van 1982)
- Die Nasionale Argief en Rekorddienswet van Suid Afrika (Wet 43 van 1996)
- ABS/ISO 27k
- Die Minimum Inligtingsekuriteitstandaarde (MISS) en/of Riglyne vir die Hantering van Geklassifiseerde Inligting (SP/2/8/1)
- Die Regulering van die Onderskepping van Kommunikasies en Voorsiening van Kommunikasieverwante Intigtingwet (Wet 70 van 2002)
- Suid-Afrikaanse Skolewet, Wet 84 van 1996 met Wysigings tot 2011

5. BELEIDSVERKLARING

5.1 Algemene Voorskrifte

5.1.1 Die HHS-Netwerk is onderhewig aan 'n breë reeks wetgewing wat telekommunikasie reguleer, insluitend, maar nie beperk is tot, die Elektroniese Kommunikasie- en Transaksiewet van 2002 en die Regulering van Onderskepping Kommunikasies en Voorsiening van Kommunikasieverwante Inligtingswet van 2002 (die Onderskeppingswet).

5.1.2 Gebruikers is aan alle verwante wetgewing en beleide wat telekommunikasie en elektroniese kommunikasiebeheer onderwerp en onderneem om ten alle tye dienooreen-komstig op te tree. Gebruikers erken dat hulle toegang tot telekommunikasie-inligtingtegnologie, insluitende e-pos en Internet wat deur die organisasie verskaf is, het. Die uitsluitlike rede vir sodanige verskaffing aan gebruikers is om hul in die uitvoering van hul dienste en verantwoordelikhede as werksfunksie of ander amptelike optrede van die HHS-Netwerk te bemagtig.

5.1.3 Gebruikers erken dat hulle geen verwagting op privaatheid het terwyl hulle enige telekommunikasietoerusting onder beskerming van die HHS-Netwerk handel en gee hiermee toestemming aan die HHS-Netwerk om t.o.v. enige elektroniese telekommunikasie, gestoorde leêrs of indirekte kommunikasie wat onder hul beheer is of was, soos deur die RICA-Wet voorgeskryf, te mag onderskep, monitor, lees, filter of andersins teen op te tree.

5.2 Gebruik van die Skool se Netwerk IT-toerusting

5.2.1 Die leerder aanvaar verantwoordelikheid vir sy/haar werkstasie en draagbare toestel.

5.2.2 Indien die toerusting gesteel, beskadig, uitgeleen of andersins nie vir normale onderrig beskikbaar is, moet dit onmiddellik aan die IT-administrateur of -intern gerapporteer word.

5.2.3 HHS-Netwerk-toerusting mag nie sonder toestemming van die Skool se Netwerk perseel verwyder word nie.

5.2.4 Geen moeite moet gespaar bly om diefstal van toerusting te verhoed nie.

5.2.5 Gebruikers moet sorg dat toerusting aan hulle toevertrou, ‘n unieke identifiseerder ontvang en volgens die Batesregister geklassifiseer is.

5.2.6 Gebruikers wat HHS-Netwerk-toerusting tuis het, sal elke poging aanwend om die toerusting volgens die *IT-Veiligheidsbeleid* te beskerm.

5.3 Gebruik van Lessenaar-Rekenaars

5.3.1 Die toestel (Chromebook of Tablet) mag nie gelyktydig aan twee of meer netwerke gekoppel wees nie.

5.3.2 Gebruikers moet met ‘n gebruikersnaam en wagwoord verskaf word om toelating tot die HHS-Netwerk te verkry.

5.3.3 Gebruikers moet wagwoorde beveilig en nie hul rekeninggeloofsbriewe met ander deel nie. Gebruikers is verantwoordelik vir die beveiliging van hul wagwoorde en rekenings.

5.3.4 Die toestel moet met die nuutste anti-virussagteware, virusdefinisies en bedryfstelsel-opgradering op datum gehou word.

5.3.5 Die gebruiker moet nie die konfigurasie van die anti-virussagteware afsit of verander nie.

5.3.6 Gebruikers sal nie enige onwettige of ongoedgekeurde sagteware op WKR-toerusting laai nie.

5.3.7 Gebruikers erken verantwoordelikheid vir enige ongemagtigde- of roofsagteware in hul besit of op toerusting aan hulle toevertrou is of deur hulle in gebruik gevind word.

5.4 E-pos

Die HHS-Netwerk ondersteun slegs die installering van goedgekeurde e-poskliënte. Gebruikers-name sal deur die HHS-Netwerk toegeken word en sal die inwendig gemagdigte e-posbenamings-konvensies volg.

5.4.1 Aanvaarbare e-Posgebruik

5.4.1.1 Kommunikasie op 'n professionelevlak.

5.4.1.2 Kort persoonlike kommunikasies wat nie op werksverantwoordelikhede inbraak maak nie.

5.4.1.3 Elektroniese boodskappe is dikwels onvoldoende in die oordra van toon en konteks. Gebruikers moet mooi besin hoe die ontvanger 'n boodskap mag interpreteer voordat dit opgestel en versend word.

5.4.2 Onaanvaarbare e-Posgebruik

5.4.2.1 Die skep en wisseling van e-poste wat as aanstootlik, teistering, onwelvoeglik, rassisties, seksisties, ouderdomdiskriminerend, pornografies of dreigend ervaar mag word.

5.4.2.2 Die skep en wisseling van inligting wat kopiereg of enige ander wet skend. Die HHS-Netwerk is nie verantwoordelik vir e-posgebruik wat die gereg oortree nie.

5.4.2.3 Die oopmaak van aanhangsels van 'n onbetroubare bron of een met 'n onverwagte onderwerpslyn.

5.4.2.4 Die stuur van inligting aan ongemagtigte persone of die skending van die Minimum Inligting Veiligheid Standaarde. Andersins met die gebruik van e-pos op 'n manier wat die HHS-Netwerk se wetlike en regulerende aanspreeklikheid verhoog.

5.4.2.5 Kommunikasies wat die HHS-Netwerk onnodiglik belas, soos bv. met die stuur van groot leêrs of verspreidingstabelle.

5.4.2.6 Die omsend van kettingbriewe of handelsaanbiedinge.

5.4.2.7 Die omsend van onbeskermde data en persoonlik uitkenbare kliënt/burger data wat Artikel 14 van die Grondwet oortree.

5.4.2.8 Die bevordering of publisering van 'n gebruiker se politieke siening, die bedryf van 'n besigheid of enige winsgewende onderneming.

5.4.2.9 Die gebruik van die e-posstelsel vir enige doeleinde of op enige manier wat moontlik die regte of belange van die HHS-Netwerk benadeel.

5.5 Internet

Die gebruik van Internet word gegun vir die uitsluitlike doel om die HHS-Netwerk se aktiwitete te ondersteun. Alle Internetgebaseerde transaksies, wat hul oorsprong in die HHS-Netwerk het, word versigtig vir oudit- en voldoeningsdoeleindes gemonitor.

5.5.1 Aanvaarbare Gebruik van die Internet

5.5.1.1 Toegang tot webgebaseerde programme en gereedskap.
5.5.1.2 Kommunikasie tussen amptenare en nie-amptenare vir besigheidsdoeleindes.
5.5.1.3 Oorsig van moontlike webblaaie vir onderrigdoeleindes.
5.5.1.4 Verwysingsregulering of tegniese inligting in lyn met posbeskrywing of amptelike funksies.
5.5.1.5 Toegang tot Regeringswebwerwe of –poorte.
5.5.1.6 Navorsing in lyn met relevante posbeskrywing of amptelike funksies.

5.5.2 Onaanvaarbare Gebruik van die Internet

Verkryging, stoor en verspreiding van onwettige data wat pornografies is of negatief op ras wys, geslag, seks, swangerskap, huwelikstatus, etniese- of sosialestatus of -agtergrond, seksuele orientasie, ouderdom, gestremdheid, geloof, gewete, kultuur, taal en geboorte, is spesifiek verbode. Die HHS-Netwerk verbied ook deelname in bedrog of die wetende verspreiding van lasterlike materiaal.

Ander aktiwiteite wat streng verbied word, sluit in, maar is nie beperk tot:

5.5.2.1 Toegang tot inligting wat nie binne die gebruiker se werkopdrag is nie. Dit sluit ongemagtigde toegang en/of die lees van HHS-Netwerk inligting, toegang tot personeelinligting en toegang tot inligting wat nie vir die behoorlike uitvoering van werksfunksies is nie.
5.5.2.2 Doelbewuste aanwys of hiperskakeling van die HHS-Netwerk webwerf met ander soortgelykes wie se inhoud teenstrydig of 'n skending van die doelwitte en beleide van die HHS-Netwerk is.
5.5.2.3 Enige optrede wat, of 'n misdaad is, of 'n misdaad aanmoedig, lei tot siviele aanspreeklikheid, of andersins enige regulasie of voorskrifte van algemene wetskending.
5.5.2.4 Die gebruik, oordrag, duplisering of vrywillige ontvangs van materiaal wat grens aan die kopiereg, handelsmerke, handelsgeheime of patentregte van enige individu of organisasie. [Amptenare moet aanvaar dat alle materiaal op die Internet kopiereg- of patentebeskerming het tensy kennisgewings dit spesifiek vryspreek.]
5.5.2.5 Oordrag van enige persoonlike, vertroulike of andersins sensitiewe inligting sonder die behoorlike beheer en uitdruklike toestemming van die relevante lasgewende partye nie.
5.5.2.6 Enige vorm van aanlyndobbel of spel.
5.5.2.7 Die gebruik van die Internet vir enige doel, of op enige wyse wat die regte, of belange van die HHS-Netwerk of WKR in enige ander omgewing mag skaad.

5.6 Inligting Beveiliging

5.6.1 Alle gebruikers van die HHS-Netwerk inligting sal die vertroulikheid, integriteit en beskikbaarheid van inligting behou.

5.6.2 Gebruikers moet verseker dat alle geheuestokke, dryf en CD's geformateer en van alle data gereinig is tot so ’n mate dat herstel van media en herwinning onmoontlik gemaak is.

5.6.3 Gebruikers moet verseker dat alle media vir die stoor van data bedoel in ‘n veilige omgewing en ’n veilige afstand van elektromagnetiese versteuring, soos telefone, wat media kan beskadig geberg word.

5.6.4 Gebruikers moet nie lêers met almal op die netwerk deel sonder gebruiker se aanmelding verifikasie toegang sekuriteit in plek dat behoorlike gebruiker aanmeldingverifikasietoe-gangsekuriteit (Logon)

5.6.5 Gebruikers moet geen ongemagtigde afskrifte of modifikasies aan die inhoud van enige HHS-Netwerkbronne maak of aanbring nie.

5.6.6 Gebruikers moet alle inligtingsbronne met veiligheid hanteer.

5.6.7 Gebruikers moet verseker dat alle inligting onder hulle beheer gerugsteun word in ooreen-stemming met die belangrikheid van die inligting van die HHS-Netwerk.

6. PRIVAATHEIDSBELEID

6.1 Die HHS-Netwerk behou die reg voor om e-pos en Internetbedrywigheid te monitor en hersien om nakoming van hierdie Beleid as ook die HHS-Netwerk se wetsgetrouheid te verseker. Gebruikers het geen verwagting tot privaatheid nie.

6.2 Met beëindiging of ontkoppeling van die HHS-Netwerk sal toegang tot e-pos en Internet belet word, insluitend die vermoë om enige boodskap in die sisteem gestoor af te laai, vorentoe te druk of te herwin, ongeag die sender of ontvanger.

6.3 Amptenare of leerders wat ‘n posbus op die HHS-Netwerk gebruik en die instansie verlaat, sal die posbus onmiddellik deur die organisasie gedeaktiveer word.

6.4 Die HHS-Netwerk behou die reg voor om enige en alle boodskappe wat gekomponeer, gestuur of ontvang is, te onderskep, te monitor, te hersien en/of te openbaar. Afsny, monitering en hersiening van boodskappe kan uitgevoer word met die hulp van inhoudfiltreringssagteware, of deur aangewese HHS-Netwerk amptenare.

6.5 Die HHS-Netwerk behou die reg voor om die aflewering van e-posboodskappe, soos toepaslik, te verander, te herlei of te sluit. Dit is nie bepaald tot:

6.5.1 Verwerping, kwarantyn of verwydering van aanhangsels en/of kwaadwillige kode uit boodskappe wat moontlik 'n bedreiging vir HHS-Network hulpbronne inhou.

6.5.2 Die verwydering van aanhangsels, soos musiek, wat as van min waarde beskou word en 'n aansienlike hulpbronkoste behels.

6.5.3 Verwerping of kwarantyn van boodskappe wat verdagte inhoud bevat.

6.5.4 Verwerping of kwarantyn van boodskappe wat aanstootlike taal bevat.

6.5.5 Herleiing van boodskappe met verdagte inhoud aan aangewese HHS-Netwerk werknemers vir handleiding hersiening.

6.5.6 Byvoeging van wettige afwysings aan boodskappe.

6.6 Elektroniese boodskappe is toelaatbaar as hoofgetuienis.

6.7 Enige inhoud wat in die e-possisteem geskep word, sal as die intellektuele eiendom van HHS-Netwerk beskou word.

7 KUBERKNOUERY

7.1 Kuberknouery is die proses om die Internet of mobiele toestelle te gebruik om enige teks of beelde te stuur en/of plaas wat bedoel is om pyn, foltering, dreigement, verleentheid van 'n ander persoon aan te rig, en sluit sulke gedrag deur middel van e-pos-, selfoon- en sms-boodskappe, kitsboodskappe, persoonlike webwerwe en/of kletskamers in.

7.2 Kuberknouery neem verskillende vorme, insluitende:

7.2.1 Kitsboodskap (IM) / SMS-teistering: stuur haatlike of dreigende boodskappe na die teiken.

7.2.2 Waarskuwingsoorloë: verslagdoening van gepleegde oortredings van diensverskaffers se terme/webwerfterme wat tot gevolg kan hê dat die teiken vanaf 'n bepaalde webwerf of sosiale network verban word.

7.2.3 Teksoorloë en teksaanvalle: die teiken word aangeval deur middel van teksboodskappe wat aan sy selfoon of e-pos gestuur word.

7.2.4 Steel van wagwoorde: voordoening as sodanige persoon en plaas dan ongepaste/ skadelike/onwettige poste via sodanige valse profiel.

7.2.5 Die stuur en plasing van vernederende foto’s of video's.

7.2.6 Uitlaating: om iemand se geheime of verleenthede aanlyn te deel.

7.2.7 Foppery: die teiken mislei om geheime of verleenthede te openbaar en dan aanlyn te plaas.

7.2.8 Uitskakeling: opsetlik en kwaadwillig iemand uitsluit van 'n aanlyn of mobiele toestel-uitsendingsgroep.

7.2.9 Bedreiging van ’n teiken met persoonlike geweld (insluitend doodsdreigemente) wat vrees of 'n oortuiging in die slagoffer kan veroorsaak dat sulke persoonlike geweld wel mag plaasvind.

7.2.10 Kubersluiping: gerapporteerde en intensiewe teistering, ontwrigting en bedreigings.

7.2.11 Internetstemming/–gradering: Wie is “Hot”? Wie is nie? Wie is die grootste “nerd” in die sesde graad? Hierdie tipe vrae versprei vinnig op die Internet-opnames, wat deur jongmense/ kinders geplaas word.

7.2.12 Plaas van regte foto’s of gedoktorde beelde van die teiken.

7.2.13 Persoonlike of intieme inligting oor die teiken deel.

7.2.14 Deel kontakbesonderhede oor die teiken, tesame met 'n suggestiewe versoeke bv. ("vir 'n goeie gesprek ..." of "Ek is geïnteresseerd in [vul die leë spasie ...]").

7.2.15 Die stuur van pornografiese en ander ongewenste e-posse en IM's: Soms sal kuberteisterers hul slagoffers aansluit vir e-posse en IM bemarkingslyste, veral op porno-webwerwe, wat daartoe lei dat die slagoffer verskeie e-posse van porno-webwerwe ontvang.

7.3 Rol van WKR

7.3.1 Die WKR streef daarna om 'n klimaat te skep waarin elke leerder akademies, sosiaal, geestelik en emosioneel kan ontwikkel. Ten einde om dit te laat gebeur, moet leerders veilig en ondersteun voel, wat insluit dat die WKR alle elemente van kuberteistering hanteer.

7.3.2 Om sulke beginsels te bevorder, het die WKR die reg om enige voorval van kuberteistering wanneer dit via die IKT-stelsels of op persoonlike toestelle voorkom wat aan die Hermanus Hoërskool Wi-Fi gekoppel word te hanteer.

7.3.3 Die WKR is geregtig om enige voorval van kuberteistering te hanteer waar:

7.3.3.1 Kuberteistering plaas vind op kampus en nie noodwendig via die IKT-sisteem, waar die kuberteisteraar/oortreder die teiken se opvoeding/skoolonderrig nadelig beïnvloed of sy leer in die klaskamer ontwrig nie. Bv. 'n leerder kan nie op skool konsentreer nie, bly toenemend afwesig van skool of tot gevegte op skool/ in die klaskamer lei.

7.3.3.2 Dit het 'n impak op die reputasie / integriteit van die WKR; 'n werknemer, leerder of ouer.

7.3.3.3 'n Leerder vertrou aan 'n onderwyser/ander leerder oor kuberteistering van kampus af of nie via die IKT-stelsel nie en die onderwyser/ander leerder is bekommerd dat so 'n kuberteistering die leerder benadeel.

8. SOSIALE MEDIA

8.1 Sosiale media is die platform wat interaktiewe deelname van gebruikers moontlik maak om inhoud en kommentaar te skep (een tot een, een tot baie en baie tot baie). Sulke kommunikasie kan via enige aantal toestelle, soos rekenaars, tabelle, slimfone ens. plaasvind. Voorbeelde sluit Facebook, Twitter, Instagram, Whatsapp, Mxit, Google+, Tumblr , ens. In.

8.2 ‘n Paar voorbeelde:

8.2.1 Blogs is kort vir "web-logs", dit is webwerwe wat as deurlopende joernale met verskeie inskrywings funksioneer. Aanlynforums laat lede toe om gesprekke te hou deur boodskappe te ruil. Tipies word inskrywings gekategoriseer met "tags" vir maklike soek. Die meeste blogs maak voorsiening vir leser se kommentaar. Voorbeelde: Blogger, WordPress, Type Pad.

8.2.2 Mikro-blogs - hierdie blogs maak voorsiening vir korter inhoudposte, gewoonlik met 'n beperkte stel getikte karakters. Mikro-blogs kan vir statusopdaterings gebruik word en om inligting vinnig aan vriende of volgelinge te kommunikeer. Hierdie word uitgestoot aan enigiemand wat ingeteken is om die opdaterings te ontvang. Voorbeelde: Twitter, Tumblr.

8.2.3 Inhoudsgemeenskappe / Mediadeling - dienste waarmee jy verskeie media kan oplaai en deel, soos foto's en video's. Byvoorbeeld: YouTube, Flickr.

8.2.4 Boekmerk van webwerwe – dienste wat u toelaat om skakels na verskillende webwerwe en bronne oor die Internet te stoor, organiseer en bestuur. Voorbeelde: Delicious, StumbleUpon, Pinterest.

8.3 Reëls vir die gebruik van die Sosiale Media soos voorgeskryf in die Sosiale Netwerkbeleid.

8.3.1 Toegang tot sosiale media is 'n voorreg en nie 'n reg nie en word volgens die uitsluitlike diskresie van die WKR vir leerders ouer as 13 toegelaat.

8.3.2 Die WKR moedig die gebruik van sosialenetwerke /-media (Twitter, Facebook, ens.) aan as 'n manier om met ander te skakel, opvoedkundige hulpbronne te deel, opvoedkundige inhoud te skep en reguleer en die klaskamerervaring te verbeter. Terwyl sosiale netwerke pret en waardevol is, is daar sekere risiko's wat in gedagte gehou moet word wanneer hierdie gereedskap gebruik word. In die sosiale mediawêreld word die lyne vervaag tussen wat publiek of privaat, persoonlik of professioneel is.

8.3.3 Gebruik goeie oordeel.

8.3.4 Ongeag privaatheidinstellings, aanvaar dat al die inligting wat jy op jou sosialenetwerk gedeel het, openbare inligting is.

8.3.5 Hanteer ander altyd op 'n respekvolle, positiewe en bedagsame manier.

8.3.6 Wees verantwoordelik en eties.

8.3.7 Tensy u spesifiek gemagtig is om u as WKR woordvoerder voor te stel, meld dat die standpunte wat in u plasings uitgespreek is, u eie is.

8.3.8 Moenie inligting publiseer, pos of vrylaat wat as vertroulik of privaat beskou word nie. As dit vertroulik lyk, is dit waarskynlik. Aanlyn "gesprekke" is nooit privaat nie.

8.3.9 Moenie jou geboortedatum, adres, selfoonnommer op enige openbare webwerf bekend maak nie.

8.3.10 Om jou veiligheid te verseker, wees versigtig oor die tipe en hoeveelheid persoonlike inligting wat jy verskaf. Vermy praat oor persoonlike skedules, situasies, jou skool en plekke van naskoolse aktiwiteite.

8.3.11 Gee NOOIT persoonlike inligting van leerders, onderwysers of ouers uit nie.

8.3.12 Moenie foto's/video's/inligting van enige skoolaktiwiteite sonder die toestemming van die WKR pos nie.

8.3.13 Moenie foto's/video's/inligting van enige leerder, ouer, onderwyser, besoeker aan die skool plaas sonder sy/haar skriftelike toestemming nie.

8.3.14 Wanneer sosiale netwerkblaaie gebruik word moet aan die bepalings en voorwaardes voldoen word.

8.3.15 Moenie lasterlike of kwaadwillige opmerkings oor die WKRHHS, enige leerder, ouer, onderwyser of ander werknemer van die WKR op enige sosiale media platform of via enige mobiele boodskap-aansoek plaas nie.

8.3.16 Moenie die WKR/HHS logo vir endossemente gebruik nie.

8.3.17 Moenie die WKR/HHS logo of enige skoolbeelde of ikonografie op persoonlike sosiale mediawerwe gebruik nie.

8.3.18 Moenie die WKR/HHS naam of logo gebruik om enige oorsaak te bevorder sonder vooraf toestemming te verkry nie.

9. PERSOOONLIKE TOESTELLE

Die gebruik van persoonlike toestelle word NIE vir opvoedkundige doeleindes toegelaat nie.

10. STOOR VAN DOKUMENTE

10.1 Leerders word voorsien van netwerkliggings waarin dokumente gestoor word en hierdie liggings word slegs verskaf vir die stoor van skoolverwante dokumente. Hierdie plekke mag nie aangewend word om enige persoonlike inligting op te stoor nie.

10.2 In die besonder mag geen persoonlike foto's, musiek en video clips op enige deel van die IKT-stelsel gestoor word sonder die toestemming van WKR/HHS nie.

11. MONITERING

11.1 As deel van die voortdurende poging om leerders te beskerm wanneer die IKT-stelsel en persoonlike toestelle gebruik word, en om te verseker dat leerders 'n positiewe en veilige ervaring het, moet die gebruiker erken dat WKR/HHS en sy verteenwoordigers enige kommunikasie kan monitor, toegang kry tot, ondersoek en onderskep op of via enige komponent van die WKR IKT-stelsel of persoonlike toestelle, deur menslike of outomatiese middele. Vir so 'n doel het WKR sagteware wat ontwerp is om elke leerder se gebruik van die IKT-stelsel, al sy/haar kommunikasie en alle gebruik van persoonlike toestelle te monitor wanneer hy aan die WKG/ HHS Wi-Fi gekoppel is.

11.2 Leerders sal geen verwagting van privaatheid hê as hulle enige komponent van die IKT-stelsel gebruik nie.

11.3 Leerders sal saamwerk met die WKR / HHS om sulke toegang te verseker en te hersien, insluitende die nodige wagwoorde. Versuim om op hierdie manier met die WKR saam te werk, kan daartoe lei dat dissiplinêre stappe geneem word.

11.4 WKR mag soms eksterne ondersoekers en/of kundiges aanstel vir die doeleindes van forensiese en ander ondersoeke na onwettige gebruik en/of toegang tot die IKT-stelsels en/of onwettige aktiwiteite wat die IKT-stelsels gebruik. Sodanige eksterne ondersoekers en/of kundiges moet toegang hê tot die leerder se kommunikasie en/of die IKT-stelsel. Geen ondersoeker/deskundige sal toegang verleen tot enige kommunikasie- en/of IKT-stelsels nie, behalwe vir die uitsluitlike doel om 'n oudit/ondersoek te doen soos beskryf/ aangedui in hierdie klousule.

12. DISSIPLINÊREPROSES

12.1 Oortreding van hierdie Beleid kan tot dissiplinêre optrede lei.

12.2 As u dink dat u die Beleid oortree het, moet u asseblief onmiddellik 'n onderwyser of die IKT-ondersteuningspersoneel in kennis stel sodat die skool die nodige stappe om die impak daarvan te verminder, kan doen.

13. KONTRAKBREUK

Waar 'n verbreking of nalatigheid i.v.m hierdie Beleid plaasgevind het, sal toepaslike dissiplinêre optrede in ooreenstemming met die relevante HHS Network-Beleid geneem word.

14. BELEIDINTREEDATUM

Die Beleid sal effektief vanaf die datum waarop dit deur die betrokke owerhede geteken is, intree.

15. BYLAAG - DEFINISIE VAN TERME

Agente: 'n Nuwe tipe sagteware wat spesiale take namens 'n gebruiker uitvoer, soos bv. soekinligting.

Vertroulike inligting: 'n Aanwysing vir inligting, waarvan die openbaarmaking HHS Netwerk of sy besigheidsaffiliasies sal beskadig.

Kritieke inligting: Enige inligting wat noodsaaklik is vir HHS Netwerk besigheidsaktiwiteite, die vernietiging, wysiging of onbeskikbaarheid daarvan, wat ernstige ontwrigting van HHS Netwerk besigheid kan veroorsaak.

Data Sekuriteit Klassifikasie: Die verwysing na "sensitiewe" data verwys na die klassifikasie van HHS Netwerk data in twee basiese kategorieë:

HHS Netwerk Eiendomsbeskrywing is inligting rakende besigheidsbedrywighede, nuwe produkte, tegnieke, voorstelle of verwante inligting wat, indien gekompromitteer, HHS Netwerk-bedrywighede ernstig sou benadeel.

HHS Netwerk Privaat is inligting wat verband hou met besigheidsaktiwiteite of individue, en is van so 'n belang vir die HHS Netwerk, of dit is so persoonlik van aard, dat onoordeelkundige vrylating nadelige uitwerking op die HHS Netwerk of die betrokke werknemer sou hê. Voorregte werknemersinligting soos salarisse en personeelrekords soos verandering versoeke is tipies van HHS Netwerk Privaatinhoud.

Verstek wagwoord: 'n Aanvanklike wagwoord uitgereik wanneer 'n nuwe gebruikers-ID uitgereik word, of 'n aanvanklike wagwoord wat deur 'n rekenaarverkoper verskaf word wanneer hardeware/ sagteware eers afgelewer word.

Laai: Die oordrag van data vanaf stelsels van 'n gasheer rekenaar (hoofraam, minirekenaar, netwerk bediener, ens.) na 'n gekoppelde werkstasie, soos 'n persoonlike rekenaar.

Eindgebruiker: 'n Gebruiker wat rekenaars gebruik om besigheidsaktiwiteite te ondersteun, wat optree as die bron of bestemming van inligting wat deur 'n rekenaarstelsel vloei.

Uitgebreide gebruikersverifikasietegniek: Enige van die verskillende prosesse wat gebruik word om die gebruikersidentifikasieproses wat deur gebruikers-ID's en vaste wagwoorde behaal is, te versterk (sien handwapens en dinamiese wagwoorde).

Brandmuur: 'n Logiese versperringstop teen rekenaargebruikers of -prosesse wat vordering by 'n sekere punt in 'n netwerk verbied of keer, tensy hierdie gebruikers of prosesse eers 'n sekuriteitstoets geslaag het (soos die verskaffing van 'n wagwoord).

Inligtingsretensieskedule: 'n Formele lys van die soort inligting wat vir argiefdoeleindes behou moet word en die tydsraamwerke wat hierdie tipe inligting moet eerbiedig.

Intekenbannier: Die aanvanklike boodskap wat aan 'n gebruiker voorgelê word wanneer hy/sy eers 'n verbinding met 'n rekenaar maak.

Intekenteks: 'n stel gestoorde instruksies wat outomaties 'n gebruiker outomaties in 'n rekenaar kan aanteken.

Meesterkopieë van sagteware: Kopieë van sagteware wat in 'n argief behou word en wat nie vir normale besigheidsaktiwiteite gebruik word nie.

Wagwoord raai-aanval: 'n Gerekenariseerde- of handleidingproses waardeur verskeie moontlike wagwoorde aan 'n rekenaar voorgelê word in 'n poging om ongemagtigde toegang te verkry.

Wagwoordherstelling: Die opdrag van 'n ander (tydelike) wagwoord wanneer 'n gebruiker sy/haar wagwoord vergeet of verloor.

Wagwoordgebaseerde toegangsbeheer: Sagteware wat op wagwoorde staatmaak as die primêre meganisme om stelselregte te beheer.

Wagwoord: Enige geheime string karakters wat gebruik word om 'n rekenaargebruiker of proses positief te identifiseer.

Positiewe identifikasie: Die proses om die identiteit van 'n rekenaargebruiker finaal vas te stel.

Privilegie: 'n Gemagtigde vermoë om 'n sekere optrede op 'n rekenaar uit te voer, soos 'n spesifieke rekenaarlêer.

Beperkte Gebied: 'n Gebied waarin sensitiewe inligting verwerk of mee gewerk word en daarom fisiese toegangsbeheer vereis.

Beperkte inligting: Besonder sensitiewe inligting, waarvan die openbaarmaking van HHS Netwerk of sy besigheidsmaatskappye ernstig beskadig word (sien vertroulike inligting).

Skermbewaarder: 'n Rekenaarprogram wat outomaties die skerm van 'n rekenaarmonitor, CRT, LCD, of Plasma na 'n sekere tydperk van geen aktiwiteit afsit.

Sekuriteitsplak: 'n Programmatuur wat gebruik word om 'n sekuriteits- of ander probleem op te los (algemeen toegepas op bedryfstelsels).

Gevoelige inligting: Enige inligting waarvan die openbaarmaking HHS Netwerk of sy sakevennote kan beskadig. Enige data gemerk as HHS Netwerk geheim of HHS Netwerk top geheim.

Gedeeldewagwoord: 'n Wagwoord wat bekend is deur en/of gebruik word deur meer as een individu.

Spesiale stelselvoorreg: Toegang stelsel regte wat die betrokke gebruiker of proses toelaat om aktiwiteite te verrig wat normaalweg nie aan ander gebruikers toegeken word nie.

Opskort van gebruikers-ID: Die proses om die voorregte wat met 'n gebruikers-ID geassosieer word, te herroep.

Stelseladministrateur: 'n Aangewese individu met spesiale voorregte op 'n veelgebruikte rekenaarstelsel, en wat by sekuriteit en ander administratiewe aangeleenthede inpas.

Oplaai: Die oordrag van data vanaf 'n gekoppelde toestel, soos 'n persoonlike rekenaar, na 'n gasheerstelsel (hoofraamwerk, minicomputer, bediener, ens.).

Gebruikers-ID's: Ook bekend as rekeninge, dit is tekenreekse wat rekenaargebruikers of rekenaarprosesse uniek identifiseer.

Waardevolle inligting: Inligting van beduidende finansiële waarde aan die Parlement of 'n ander party.

Verifieer sekuriteitstatus: Die proses waardeur kontroles getoon word, is beide behoorlik geïnstalleer en behoorlik bedryf.

Virus: 'n Parasitiese sagtewareprogram wat toegerus is met die hersieningsmetodiek wat versprei deur 'n rekenaar of netwerk deur homself te verbind of ander sagteware of diskette te besmet. 'n Wurm is 'n soortgelyke program wat oor ‘n network versprei en kopieë maak.

Virus skermsagteware: Kommersiële verkrygbare sagteware wat vir sekere bit-patrone of ander getuienis van rekenaarvirusinfeksies soek.