HIC Anti-Virus and Endpoint Data Protection Policy

Overview

The purpose of this policy is to provide guidelines for acceptable use and protection measures for end point devices, specifically AV tools and usage, as well as establishing the protocols for data protection at the end point. Users who are assigned a corporate mobile and computing devices or are approved for accessing HIC resources from a BYOD (Bring Your Own Device) or tablet are required to agree and comply by signing the separate Policy supplement found attached to this document.

Scope

This policy applies to all employees who have been assigned any corporate laptop, workstation, cell phone, broadband device, or company issued VPN phones, or approved Bring Your Own Devices (BYOD). All end point devices will be required to have onboard antivirus, antimalware protection that will be pushed, monitored, maintained and managed by HIC IT. Additionally, in conjunction with the corporate standard for end point security AV, all end point devices that house ANY HIC data, or any of its subsidiaries will be required to have IT issued encryption solutions installed and actively working on the end point. End users will not have control or say in the management, maintenance or administration of these IT implements.

Integrity

This policy has been designed to maintain the integrity of all of HIC's PHI Data as it pertains to our customers, 3rd party entities and minimum compliance standards set forth by our governing agencies and our Board of Directors and shareholders. HIC will maintain a zero tolerance enforcement of this policy. Please make close reference to the 'Special Conditions' clause of this policy below and if you have questions or concerns please address them to your management chain. Please note, however, that exceptions to this policy and its special conditions will not be entertained. We understand that this policy may seem heavy handed and we understand that you may be passionate about an alternative position. In these cases, we encourage you to submit an appropriate business and use case that outlines and clearly expresses the financial benefit in direct comparison of the associated risk value/cost to the HIC Organization. Any submittals will be forwarded to the Executive team for review and follow-up.

Corporate End Points

1. All Corporate End Points should be limited to proper business use. HIC mandates that all end points interacting with the HIC IT Infrastructure will have the ESET Smart Security End Point Solution.
2. All HIC Corporate End Points interacting with HIC IT Infrastructure will have Deslock Encryption protection by ESET installed.
3. All HIC Peripherals that store and/or transmit data (ie: Thumb Drives, Memory Sticks, Memory Cards) will be subject to this policy as well.

BYOD Bring Your Own Device

1. Per HIC Mobility Policy: HIC currently supports BYOD for approved employees using most Android and iOS devices. HIC will only support devices left in their OEM, Factory, or Carrier-Specific Firmware. Rooted, Jail-broken or 3rd party ROMS/Firmware cannot be enrolled in this program.

2. All BYOD devices will be subject to the standards of data protection as outlined in the Corporate End Points section of this policy.
3. HIC IT will install an MDM solution on approved BYOD devices. Further, HIC Employees consent by virtue of signature below that HIC IT will have manage, monitor and update push control to approved BYOD devices – up to and including remote wipe in the event of a loss of the BYOD device.

Antivirus Skepticism and End Point Protection – HIC's Position

HIC recognizes that there is much debate amongst security professionals as to the effectiveness and relevance of Antivirus in the modern technology landscape. HIC likens Antivirus/Antimalware protection on the endpoint as to physical locks on doors and windows in the physical security realm. Antivirus/Antimalware software on the end point serves as a critical component of basic cyber hygiene, much like physical locks on doors and windows keep burglars at bay but are not the only implements to prevent a burglary. However, they are certainly a frontline deterrent. Further, as the industry advances and the cybercriminals become more and more savvy with methods to thwart traditional signature based AV models, HIC has selected next gen AV and encryption solutions that incorporate heuristics, machine learning and artificial intelligence technologies into the engine, in addition to a vast global signature dataset that cultivates threat information from around the globe in real-time. This all combined works to identify and prevent malware intrusion in a zero-hour model. Combine this with our approach to protecting data on all endpoints with proper encryption technologies deployed across all environments and actively monitored by the HIC Information Security team

HIC AV & Data Protection Policy Supplement

As an HIC employee, I acknowledge and agree:

1. HIC will provide antivirus/antimalware solutions for all end point devices.

2. HIC will provide End Point Encryption solutions for all Endpoint devices.

3. I understand that if I am granted BYOD privileges, HIC will install these tools on my BYOD Device as well as a remote MDM solution that will enable HIC IT to access, monitor and manage any and all HIC Data assets on my personal device. Further, if a breach is detected or if my device is reported lost or stolen, HIC IT will initiate remote wipe.

4. Any violations of this policy, including tampering with end point AV and Encryption solutions or attempting to disable, neutralize or remove HIC AV and Encryption implements will result in corrective action up to and including immediate termination of employment.

I________________________, have read and accept the terms and conditions of the HIC Mobile Device Policy listed above.

Employee Signature: ____

Date: _____________