WEST VIRGINIA CODE: §21-5H-1

§21-5H-1. Employer access to employee or potential employee personal accounts prohibited.

(a) An employer shall not do any of the following:

(1) Request, require or coerce an employee or a potential employee to disclose a username and password, password or any other authentication information that allows access to the employee or potential employee's personal account;

(2) Request, require or coerce an employee or a potential employee to access the employee or the potential employee’s personal account in the presence of the employer; or

(3) Compel an employee or potential employee to add the employer or an employment agency to their list of contacts that enable the contacts to access a personal account.

(b) Nothing in this section prevents an employer from:

(1) Accessing information about an employee or potential employee that is publicly available;

(2) Complying with applicable laws, rules or regulations;

(3) Requiring an employee to disclose a username or password or similar authentication information for the purpose of accessing:

(A) An employer-issued electronic device; or

(B) An account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes;

(4) Conducting an investigation or requiring an employee to cooperate in an investigation. The employer may require an employee to share the content that has been reported to make a factual determination, if the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information or financial data, to an employee's personal account;

(5) Prohibiting an employee or potential employee from using a personal account during employment hours, while on employer time or for business purposes; or

(6) Requesting an employee to share specific content regarding a personal account for the purposes of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct.

(c) If an employer inadvertently receives the username, password or any other authentication information that would enable the employer to gain access to the employee or

potential employee's personal account through the use of an otherwise lawful technology that monitors the employer's network or employer-provided electronic devices for network security or data confidentiality purposes, then the employer is not liable for having that information, unless the employer:

(1) Uses that information, or enables a third party to use that information, to access the employee or potential employee's personal account;

(2) After the employer becomes aware that that information was received, does not delete the information as soon as is reasonably practicable, unless that information is being retained by the employer in connection with an ongoing investigation of an actual or suspected breach of the computer, network or data security. Where an employer knows or, through reasonable efforts, should be aware that its network monitoring technology is likely inadvertently to receive such information, the employer shall make reasonable efforts to secure that information.

(d) Nothing in this section diminishes the authority and obligation of an employer to investigate complaints, allegations or the occurrence of sexual, racial, or other harassment as provided in this code.

(e) As used in this section, "personal account" means an account, service or profile on a social networking website that is used by an employee or potential employee exclusively for personal communications unrelated to any business purposes of the employer.