U.S. Customs and Border Protection
Operational Use of Social Media
Rules of Behavior

The following rules of behavior apply to all U.S. Customs and Border Protection (CBP) employees, contractors, and persons using CBP systems in furtherance of the CBP mission with access to social media sites and the public internet for the purposes of overseeing or conducting operational activities related to the mission of CBP. These activities may include, but are not limited to: determining admissibility, identity resolution, reconciling screening and targeting matches, counter-terrorism investigations, counter-narcotics investigations, smuggling investigations, trade and credential fraud investigations, interdictions, border and event security, enhancing general, operational awareness, and assisting in making benefit, personnel, or suitability determinations. These rules of behavior are separate and apart from those rules of behavior which cover accessing social media sites and the public internet for the purpose of communications and outreach with the public.

1. **Social Media Access, Generally:**

   a. I understand that all activities of accessing restricted internet sites or access to social media sites will be in accordance with applicable law and DHS and CBP guidance.

   b. I understand that my access to social media under these specific rules of behavior does not include conducting communications and outreach with the public, and in connection with the Office of Public Affairs as directed in CBP Directive 5410-001B, Office of Public Affairs Roles, Functions and Responsibilities.

   c. I will only access those sites for which I require access to perform mission-related tasks as part of my official duties and for purposes that are authorized by statute, executive order, regulation, or policy. I will not attempt to access sites or perform actions that I am not authorized to access or perform.

   d. I understand that I must complete all required privacy training prior to receiving access to social media sites and that I will complete annual refresher training as long as access is still needed and approved by a Template.

   e. I understand that my access requirements will be reviewed on an annual basis and that my access can be terminated at any time if it is no longer needed due to a change in official duties, if I am no longer authorized to conduct activities requiring the access, if I am serving a suspension due to misconduct,, if I am under a suspension of law enforcement authority, if I separate from CBP, or if I misuse my access.

2. **Overt Operational Use of Social Media and the Public Internet (Overt Research, Monitoring, and Engagement):**

   a. I will use only government-issued equipment, internet connections authorized to access social media through the DHS/CBP network (i.e., no "stand-alone" connections), government-approved accounts and government-approved email addresses when engaging in the overt operational use of social media and the public internet on behalf of CBP.

   b. I will only use screen names or identities that indicate an official DHS or CBP affiliation.

   c. I will not engage in the use of social media on government equipment or use any account created on behalf of CBP, for unofficial purposes.

   d. I will not use vulgar or abusive language, engage in personal attacks of any kind, or use offensive terms targeting individuals or groups while using social media or the public internet on behalf of DHS.

   e. I will not knowingly endorse commercial products, services or entities, nor will I knowingly endorse political parties, candidates or groups while using social media or the public internet on behalf of DHS.[1]

   f. I will not lobby members of Congress using DHS or any other appropriated resource via social media or the public internet.

   g. I will not use government resources to foster commercial interests or for individual profit.

   h. I will log off of or otherwise restrict access to any social media session when I am not personally attending to it.

3. **Data Protection for Overt Use:**

   a. I will not access information that is not publicly available, without consent.

   b. I will not interact with individuals who post the information, unless there is a specific and clearly articulated operational necessity to interact with individuals who post the information as defined in my authorized mission responsibilities.

---

[1] 'Knowingly' is included here because there is the possibility on social media sites like Facebook that one may be trying to click on another item and unknowingly click on a commercial product or political candidate, thereby endorsing the product or the political candidate. (b) (7)(E) [redacted]

c. I will only use the minimum amount of personally identifiable information (PII) necessary for the defined operational use of social media or the public internet.

d. I will protect any PII in accordance with the Privacy Act (where applicable) and DHS and CBP privacy policy (e.g., PII obtained from a SORN and disclosed for a use in research, monitoring, or engagement will be accounted for on a DHS-191).

e. I will not search social media sites or the public internet for or by PII unless this search is necessary for the purpose defined by my authorized operational use of social media.

f. I will not access or post classified or otherwise protected information (e.g. For Official Use Only (FOUO)) using social media or the public internet (e.g., (b) (7)(E)).

g. I will document my operational use of social media, including date, site(s) accessed, information collected, information disclosed for purposes of access, and how it was used in the same manner that CBP would document information collected during each of its operational activities.

4. **Undercover Operational Use of Social Media and the Public Internet (Masked Monitoring and Undercover Engagement):**

a. I will use government-issued equipment, internet connections authorized to access social media through the DHS/CBP network (i.e., no "stand-alone" connections), government-approved accounts and government-approved email addresses, unless authorized by the terms of my assigned mission responsibilities, when engaging in the undercover operational use of social media and the public internet on behalf of CBP.

b. I will not engage in use of social media on government equipment or use any account created on behalf of CBP for unofficial purposes.

c. I will refrain from using vulgar or abusive language, engaging in personal attacks of any kind, or using offensive terms targeting individuals or groups while using social media or the public internet, unless it is necessary as defined by the scope of my masked or assumed identity in the context of my authorized mission responsibilities.

d. I will not knowingly endorse commercial products, services or entities, nor will I knowingly endorse political parties, candidates or groups while using social

media or the public internet on behalf of DHS, unless authorized by the terms of the SMOUT for my undercover engagement.[2]

e. I will not lobby members of Congress using DHS or any other appropriated resource via social media or the public internet, unless authorized by the terms of the SMOUT for my undercover engagement.

f. I will not use government resources to foster commercial interests or for the appearance of individual profit, unless authorized by the terms of the SMOUT for my undercover engagement.

g. I will log off of or otherwise restrict access to any social media session when I am not personally attending to it.

5. **Data Protection for Undercover Use:**

a. I will not access information that is not publicly available, without consent, unless authorized in the execution of the terms of my assigned mission responsibilities.

b. I will not interact with individuals who post the information, unless there is a specific and clearly articulated operational necessity to interact with individuals who post the information as defined in my authorized mission responsibilities.

c. I will only use the minimum amount of personally identifiable information (PII) necessary for the defined operational use of social media or the public internet.

d. I will protect any PII in accordance with the Privacy Act (where applicable) and DHS and CBP privacy policy (e.g., PII obtained from a SORN and disclosed for a use in monitoring or engagement will be accounted for on a DHS-191).

e. I will not search social media sites or the public internet for or using PII unless this search is necessary for the purpose defined by my authorized operational use of social media.

f. I will not access or post classified or otherwise protected information (e.g., FOUO) using social media or the public internet (e.g., (b) (7)(E)).

g. I will document my operational use of social media, including date, site(s) accessed, information collected, and how it was used in the same manner that

---

[2] 'Knowingly' is included here because there is the possibility on social media sites like Facebook that one may be trying to click on another item and unknowingly click on a commercial product or political candidate, thereby endorsing the product or the political candidate. (b) (7)(E)

CBP would document information collected during each of its operational activities.

6. **Incident Reporting:**

- I will promptly report suspected or confirmed IT security incidents (e.g., (b) (7)(E)), and per the DHS Handbook for Safeguarding Sensitive PII and the Privacy Incident Handling Guide (PIHG), report any privacy incidents (e.g., loss or compromise of sensitive PII) to the DHS IT Help Desk at (b) (7)(E) (b) (7)(E) and my supervisor.

7. **Accountability:**

a. I understand that I have no expectation of privacy while using government Information Technology (IT) systems or any accounts created on behalf of CBP or in furtherance of CBP's mission.

b. I understand that I will be held accountable for my actions while accessing and using government IT systems and social media sites and may face disciplinary action and/or criminal or civil prosecution for misuse. Additionally, misuse may lead to removal from position and/or termination.

Acknowledgment Statement

I acknowledge that I have read the rules of behavior; I understand them, and I will comply with them. I understand that failure to comply with these rules could result in verbal or written warning, removal of access to social media on behalf of CBP, reassignment to other duties, criminal or civil prosecution, or termination.

_____ _____

Employee Signature **Date**

Participating in the CBP Operational Use of Social Media Training is required and serves as acknowledgement and acceptance of these Rules of Behavior.

Date Training Completed:_____

Upon completing the signature, date, and training completion date portion, submit this to the Privacy and Diversity Office at privacy.cbp@cbp.dhs.gov.