**[Company] Electronic Communications Monitoring Policy**

**[Date]**

1. **Policy Overview**

The purpose of this Electronic Communications Monitoring Policy (ECMP) is to delineate the procedures established by [Company] and the entities that it controls (together, the “Company”) for the monitoring of electronic communications with persons and entities identified on Schedule 1 of [FOCI Action Plan Name], to include each entity’s employees, officers, directors, representatives, and agents (together, “Covered Persons,” and individually, a “Covered Person”) to provide assurance that electronic communications are not used by any of the Covered Persons to access classified information, export-controlled information, or controlled unclassified information in the possession of the Company or to adversely affect the policies and practices of the Company in its performance of classified contracts. These procedures and forms are for mandatory use immediately in accordance with the National Industrial Security Program Operating Manual Rule (“NISPOM Rule”), 32 C.F.R. Part 117.

This ECMP applies to all personnel of the Company (including their directors, officers, employees, representatives and agents) and is applicable to all electronic communications (e.g., telephone, cell phone, fax, email, text messaging) with Covered Persons.

This ECMP shall be implemented by the Corporate Facility Security Officer (“FSO”), in coordination with the corporate Insider Threat Program Senior Official (ITPSO) and Chief Information Security Officer (CISO). The Company’s Board of Directors shall designate a cleared member (or members) of the Board to oversee the implementation and efficacy of this ECMP. On at least a quarterly and annual basis, the FSO shall provide reports to such member(s) relating to the implementation of this policy, including audits and findings relating to electronic communications with Covered Persons.

1. **Electronic Communication (Generally)**
2. Scope: All electronic communications between Company personnel and the Covered Persons, if any, are subject to monitoring to ensure that electronic communications are not used to: (a) transmit or gain access to classified information or controlled unclassified information without an authorization (license, agreement, exception, exemption); or (b) adversely affect the policies and practices of the Company in its performance of classified contracts. Specific monitoring programs for computer communications are set forth below.
3. Monitoring Responsibility:
   1. The FSO has responsibility for monitoring computer communications.
4. **Email Communication**
5. Email Connection and Usage:
   1. [Describe the programs or systems the Company will be utilizing for email communications, to include protection methods utilized. For example, firewalls, physical and logical separation, virus protection, etc…]
   2. [Describe how end-users will access their email (e.g., desktops, laptops, mobile devices, web-based, etc…) and the authentication methods for access.]
   3. [Describe how the Company conducts back-ups of email messages to include media used, server locations, frequency of back-up, and retention duration]
   4. [Describe policy and process on Company’s actions during a data spill regarding classified information or export-controlled information; to include data spills on mobile devices.]
6. Monitoring Procedures
   1. The Company will implement the following program to ensure that email communications are not used to: (a) transmit or gain access to classified information or controlled unclassified information without an authorization (license, agreement, exception, exemption); or (b) adversely affect the policies and practices of the Company in its performance of classified contracts.
   2. Company personnel are required to report to the FSO any email communications with a Covered Person, if any of these communications involved classified, export-controlled, or unauthorized controlled unclassified information or an attempt to adversely affect the policies and practices of the Company in its performance of classified contracts.
   3. The Company will perform quarterly searches on the previous quarter’s [Email Program or System] journal archives against the email address / domain name associated with Covered Persons by Company personnel. These searches will be stored in a separate instance and a sample will be reviewed by the FSO or other designated person to validate that no communications with Covered Persons were reportable in accordance with the preceding subparagraph. The size and frequency of, and the employees included in, the sample will be determined using a risk management approach. More frequent sampling will be performed for employees who serve as Key Management Personnel (KMPs); possess U.S. Government personnel security clearances (PCLs); have access to classified, export-controlled, or controlled unclassified information; perform on classified contracts; or work within cleared sites.
   4. The FSO will ensure that annual training is conducted for personnel who serve as KMPs; possess U.S. Government PCLs, have access to classified, export-controlled, or controlled unclassified information; perform on classified contracts; or work within cleared sites to confirm that they understand their obligations and that computer communications are not used to gain access to classified, export-controlled, or controlled unclassified information or adversely affect the policies and practices of the Company in its performance of classified contracts.
   5. As necessary, the FSO staff will conduct follow up interviews to address any security or policy-related concerns as it relates to the scope of this policy. The FSO shall, as necessary, escalate any security or policy-related concerns to the designated member(s) of the Board for further consideration and determination.
   6. The FSO will write and submit a quarterly and annual report to the designated member(s) of the Board detailing the review of targeted searching of captured emails, and findings.
   7. All logs, reports, and related documents will be retained by the FSO for review by the designated member(s) of the Board and DCSA until the later of a DCSA inspection or 12 months.
   8. Company personnel will be educated annually on the requirements set forth in this section.
7. Reporting Requirement: If during the review, the FSO or other designated person discovers the improper use of email communications, the discovery will be reported to the designated member(s) of the Board, and if validated, to DCSA.
8. **Instant Messaging and Texting**
9. Services: [Describe the Programs or Systems the Company will be utilizing for instant messaging and texting, both internally and externally]
10. Monitoring Procedures
    1. The Company will implement the following program to ensure that instant messaging or texting communications are not used to: (a) transmit or gain access to classified information, export-controlled, or controlled unclassified information without an authorization (license, agreement, exception, exemption); or (b) adversely affect the policies and practices of the Company in its performance of classified contracts.
    2. To the extent that instant messaging or texting applications rely on Company-owned network connections, those communications will be reviewed and monitored in the same manner as described for email, above.
    3. To monitor instant messaging or texting communications that do not rely on Company-owned network connections, the FSO will routinely issue a survey to a sample of Company employees to determine whether employees have had such communications with a Covered Person, and if so, the nature and extent of those communications, including to confirm that those communications have not involved classified, export-controlled, or unauthorized controlled unclassified information or an attempt to adversely affect the policies and practices of the Company in its performance of classified contracts, which is strictly prohibited. The size and frequency of, and the employees included in, the sample will be determined using a risk management approach. More frequent sampling will be performed for employees who serve as KMPs; possess U.S. Government security clearances; have access to classified, export-controlled, or controlled unclassified information; perform on classified contracts; or work within cleared sites. The FSO will perform follow-up interviews with Company employees as necessary.
    4. The FSO will ensure that annual training is conducted for personnel who serve as KMPs; possess U.S. Government security clearances; have access to classified export-controlled, or controlled unclassified information; perform on classified contracts; or work within cleared sites to confirm that they understand their obligations and that computer communications are not used to gain access to classified, export-controlled, or controlled unclassified information; or adversely affect the policies and practices of the Company in its performance of classified contracts.
    5. As necessary, the FSO staff will conduct follow up interviews to address any security or policy-related concerns as it relates to the scope of this policy. The FSO shall, as necessary, escalate any security or policy-related concerns to the designated member(s) of the Board for further consideration and determination.
    6. The FSO will write and submit a quarterly and annual report to the designated member(s) of the Board detailing the review of instant messaging and texting, and findings.
    7. All logs, reports, and related documents will be retained by the FSO for review by the designated member(s) of the Board and DCSA until the later of a DCSA inspection or 12 months.
    8. Company personnel will be educated annually on the requirements set forth in this section.
11. Reporting Requirement: If during the review, the FSO or other designated person discovers the improper use of instant messaging or texting communications, the discovery will be reported to the designated member(s) of the Board, and if validated, to DCSA.
12. **Social Networking, Web-Based Email, File Sharing, Collaboration Tools**
13. Social Networking: [Describe Company’s policy on using social networking sites (Facebook, LinkedIn, Instagram, TikTok, Twitter, etc…) and how Company will be providing oversight over its usage.]
14. External Web-Based Email: [Describe Company’s policy on using external Web-based email (e.g., Gmail, Yahoo!, Outlook, AOL, etc…) and how Company will be providing oversight over its usage.]
15. File Sharing: [Describe Company’s policy and usage of file sharing (e.g., FTP, SharePoint, Google Drive, Dropbox, SugarSync, etc…) and how Company will be providing oversight over its usage.]
16. Collaboration Tools: [Describe Company’s policy and usage of virtual/online collaboration tools (Zoom, Microsoft Teams, Google Meet, Slack, BlueJeans, etc…) and how Company will be providing oversight over its usage.]
17. **Facsimile**
18. Facsimile: [Describe how the Company will maintain a log to reflect telephone activity between it and the Covered Persons: how the log will be reviewed; how the log will include the Name, Position/Title of the Individual maintaining the log; the Name, Position/Title of the individual parties to the fax; and brief remarks that reflect the general topic of the fax.]
19. **Policy Requirement**

To ensure that the Company complies with U.S. Government requirements, the compliance of all Company employees with this ECMP is required. Violations of these procedures can result in disciplinary action up to and including termination.

Please contact the Corporate FSO [Name, email, phone] if you have any questions.