NATO COMMUNICATION AND INFORMATION SYSTEMS GROUP

Mons - Belgium

NCISG/CG/SWMO/22-4186 16 March 2022

NCISG DIRECTIVE 025-003

TELEWORKING DIRECTIVE

REFERENCES: See Annex E.

1. **Status.** This is a new NCISG directive.

2. **Purpose.** The purpose of this directive is to direct and guide the teleworking environment available for military and NATO civilian personnel employed at the NCISG (supporting teleworkers away from normal duty locations) and this under normal and crisis conditions.

3. **Applicability.** This directive is applicable to all NCISG military and civilian staff members. For military personnel, this directive is not to apply when in contradiction with national legislations, and National Military Representatives (NMRs) are to be consulted prior to concluding any teleworking agreement affecting military personnel.

4. **Publication Updates.** Updates are authorized when approved by the Deputy Commander/Chief of Staff (DCOM/COS) NCISG. An assessment for a revision is to be carried out not later than two years after the release date of this publication.

5. **Proponent.** The proponent for this directive is DCOM/COS office.

FOR THE COMMANDER NATO CIS GROUP:

Luigi Carpineto
Brigadier General, ITA Army
Deputy Commander/Chief of Staff

NCISG, CG, SWMO
7010 Mons, Belgium
Office : +32 65 446203
Mobile :

NCN 254-3854
Fax : +32 65 443854 (Registry)
functional mailbox@ncisg.nato.int

TABLE OF CONTENTS

ANNEXES:

A. Teleworking Agreement – Template.
B. Guidance on the Security of NATO Information when Teleworking.
C. NU Portal Procedures.
D. Best Teleworking Practices.
E. References.
F. Health and Safety Guidelines on the Teleworking.

CHAPTER 1 - GENERAL CONSIDERATIONS

1-1. **Teleworking.** NCISG teleworking allows for organising, managing oversight and creates a controlled environment for carrying out work in an Alternate Duty Location (ADL). The main aim of teleworking is to maintain effective support to operational requirements in times of peace and in crisis whilst away from the duty location.

1-2. **General provisions**. The following aspects of teleworking are covered in this directive:

a. Teleworking arrangements requested by the teleworker;

b. Teleworking requirements imposed by their Division Head;

c. NCISG (HQ, NSBs, M&S Coy's, DCMs) - wide teleworking arrangements brought on as part of addressing consequences of an emergency or business continuity measure.

1-3. Staff members may request or may be required to telework, as long as their tasks, as decided by their line of management, can be performed remotely and they are equipped with appropriate tools and technologies compatible with all NATO security arrangements in terms of means and capabilities. A minimum CIS recommended baseline for tools is to be met depending on the teleworking arrangement. More details can be found in Chapter 2, point 2.6.

1-4. **Definitions**

a. **Teleworking:** Teleworking occurs when information and communication technologies are applied to enable work to be done at a distance from the normal workplace, during working hours. Performing duties while on mission is not considered to be teleworking.

b. **Teleworker.** Includes NCISG military and civilian staff members who are working from an Alternative Duty Location and communicates with their office by phone, e-mail or internet.

c. **Alternative Duty Location.** Teleworking is to be performed from the worker's local residence or from the individual's home residence located within one of the NATO member states. The teleworker must be within recall distance of the HQ and be able to be present within a maximum time of 2 hours, except in case of Emergency Teleworking (see 2-5). Furthermore, there may be exceptional circumstances authorized by the Division Head/equivalent authority[1] where the maximum time to be present in the HQ may be adapted (increased, decreased or waived) and teleworking may also be performed in a specified location away from the staff member's local or home residence as long as this remains in the territory of a Member State of the Organization.

[1] Equivalent Authority is defined as NSB Commander for the NSB Staff and M&S Coy and DCM Commanders for DCMs; NSB Commanders may decide to delegate this authority to Section Heads/M&S Company Commander

d. **Teleworking Agreement.** An agreement, establishing the duration, termination, location and type of teleworking, as well as the minimum presence in the office, will be signed between the teleworker, their Division Head/equivalent authority and NCISG J1 or NSB S1 level. A teleworking agreement template can be found at Annex A.

e. **Working hours.** Working hours will be maintained as established in NCISG Directive (ND) 040-010, Working Hours, unless the direct supervisor establishes otherwise.

f. **Travel on Duty:** In the event of travel on duty as provided for in Article 40 of the NCPR, individuals authorised to telework, may, with the agreement of the supervisor, fund manager and NCISG J8 be authorised to start their journey from the place in which they telework. In such cases, the expenses incurred shall be paid or reimbursed from the teleworking location only insomuch as they do not exceed the reimbursement that would have been applicable had the journey started from the duty station.

1-5. Principles governing teleworking

a. **Security.** The Security Directives at References D and E, together with further guidance provided in Annex B, provide direction on the handling and hand-carriage of both electronic data and paper documents that shall apply when teleworking. During the teleworking period, the teleworker remains subject to all relevant NATO applicable regulations regarding handling and use of NATO information, as well as, all their national laws regarding the awarding and renewal of a NATO Security Clearance.

b. **Integrity and Loyalty**. During the teleworking period, the teleworker remains subject to the NCPR applicable regulations, the NATO Code of Conduct, the Standards of Conduct (AD 040-007, Reference D) and the signed loyalty declaration.

c. **Chain of Command.** The chain of command remains unaltered. NATO Staff shall avoid any action or activity, which may reflect adversely on their position or on the good reputation of the Organization.

d. **Employment Conditions.** The employment conditions will remain the same, but specific complementary, collective and/or individual teleworking instructions may be implemented to take into account the particularities of teleworking, for instance: working with sensitive information from non-security accredited locations.

e. **Voluntary and Exceptional Arrangements.** Teleworking is based on a voluntary, mutually agreed Arrangement (i.e. between both the teleworker and the Division Head/equivalent authority), although in special circumstances it may be directed. Teleworking may be required as a part of the employees job description. Unless teleworking is imposed as part of a response to an emergency, and if it is not part of the teleworker's job description, the employee can refuse to opt out of teleworking without it being a reason for termination of their employment within the organisation.

f. **Data protection.**

(1) AD 015-026, ACO Data Protection Policy (Reference K) remains the principle regulation to address data protection measures within NCISG.

(2) NCISG is responsible for taking the appropriate measures, particularly regarding software and procedures, to ensure the adequate protection of data used and processes employed by the teleworker for professional purposes.

(3) NCISG J2/6 Divisional Security Officer or Battalion/DCM Security Officer is to inform and control the teleworker's cognisance of the relevant NATO regulations on data protection as well as their responsibility to comply with them, in particular relating to the restriction on the use of IT equipment and the consequences of non-compliance with this restriction. NCISG J2/6 Divisional Security Officer or Battalion/DCM Security Officer provides safety information on teleworking (briefing) prior to the teleworker signing the Teleworking Agreement. The Teleworker will sign a form (list form) of consent to confirm their understanding of the safety principles.

g. **Privacy.** NCISG shall respect the privacy of the teleworker. Any control or monitoring systems put in place shall be proportionate to the data protection objective and be mentioned within the teleworking agreement (list agreement).

h. **Health and Safety.** The Head of NATO Body, as per Article 16 of the NCPR, remains responsible for ensuring that there are adequate health and safety conditions at the place of work in the office. The teleworker is to ensure that there are no risks or hazards that could impede their teleworking capabilities in the approved ADL, similar to that of working within the office. Health and Safety will be further developed in separate document Annex F: "Health and Safety Guidelines on Teleworking".

1-6. **Termination.** Teleworking may be ended by reaching the deadline set out in the teleworking agreement, by decision of the workers' Division Head, when the circumstances that allowed the teleworking change or cease to exist, if the performance review is not satisfactory or if the conditions that triggered a NCISG Business Continuity Plan are lifted by NCISG Chain of Command.

CHAPTER 2 - FORMS OF TELEWORKING

NCISG may authorise the following types of teleworking: short-term teleworking, long-term teleworking, regular teleworking, occasional/ad hoc teleworking and emergency teleworking. There are three forms of teleworking for the staff's choice/initiative requiring a signed teleworking agreement. The emergency teleworking results from a formal order or imposed by the Host nation. In this case and for occasional/ad hoc teleworking, there is no requirement for a signed teleworking agreement.

2-1. **Short-term Teleworking** is characterised as follows:

a. Initiated by the worker or the Division Head/equivalent authority.

b. Only for a period of a maximum of two (2) consecutive weeks, performed from the worker's ADL, followed by physical presence at NCISG.

c. Presence in the office: The worker shall be at least 1 full day present in the office for each week of teleworking. This presence in the office can be adapted (increased, decreased or waived by Division Head) without having to amend the teleworking agreement. Changes to presence arrangements will be documented by an email and followed by an acknowledgment of receipt by the teleworkers' Division Head.

d. A teleworking agreement shall be signed by the requestor, their Division Head/equivalent authority and NCISG J1/NSB S1.

e. Maximum total duration: 12 non-consecutive weeks per calendar year.

f. If the short-term teleworking is to be extended for more than two (2) weeks, then it will become a long-term teleworking agreement (see 2-2) which will have to be approved and signed.

2-2. **Long-term Teleworking** will have the following characteristics:

a. Initiated by the worker or the Division Head/equivalent authority.

b. Long-term Teleworking will be stablished for a period between 20 up to 60 (working) days, performed from the worker's ADL.

c. Presence in the office: The worker shall be at least one full day present in the office for each week of teleworking. This presence in the office can be adapted (increased, decreased or waived by Division Head/equivalent authority) without having to amend the teleworking agreement. Changes to presence arrangements will be documented by an email and followed by an acknowledgment of receipt by the teleworkers' Division Head.

d. A teleworking agreement shall be signed by the requestor, their Division Head/equivalent authority and NCISG J1/NSB S1.

e. Maximum total duration: 60 days, or 12 non-consecutive weeks, per calendar year.

2-3. Occasional/ ad Hoc Teleworking

a. Initiated voluntarily by the worker or the Division Head/equivalent authority. Must be requested three days in advance. The First Line Supervisor has to accept the request.

b. For a consecutive period of five working days or less per month, performed from the worker's ADL.

c. Presence in the office: No presence required.

d. Teleworking agreement signature is not required, but approval by Division Head/equivalent authority is required.

e. Maximum total duration: 6 times/per calendar year.

2-4. Regular Teleworking

a. Initiated voluntarily by the worker or the Division Head.

b. For a consecutive period of up to 6 months. The ratio between teleworking and office working must not exceed 50:50.

c. Teleworking should be performed from the worker's ADL.

d. A minimum presence of 2 days in the office is required. This presence in the office can be adapted (increased, decreased or waived by the Division Head/equivalent authority) without a need to amend the teleworking agreement. Changes to Presence arrangements will be documented by an email and followed by an acknowledgment of receipt by the teleworkers Division Head. The Regular teleworking agreement can be reconducted for the same period of time by mutual agreement.

e. A teleworking agreement shall be signed by the requestor, his Division Head/equivalent authority and NCISG J1/NSB S1.

2-5. Emergency Teleworking

a. Initiated by a formal Order or email or imposed by the Division Head/equivalent authority (e.g. brought on as part of addressing consequences of an emergency or business continuity measure).

b. Duration, rotation and minimal presence in the office in accordance with the Order and divisions Direction and Guidance. Emergency teleworking will supersede extant teleworking agreements.

c. A teleworking agreement is not required.

2-6. Table summarizing the differences between the type of Teleworking

Types of teleworking	Originator/ initiator	Duration	Minimum present in the office	Max. total duration	Contract type	Min. set of CIS requirements*
Short-term	Initiated by the worker or the Division Head	Max. 2 consecutive weeks	At least 1 full day present in office for each week	12 non-consecutive weeks per calendar year	Written agreement	Vasco token, NU Polycom and DNBL from a private device
Long-term		Between 20 up to 60 working days (3 calendar months)		60 days per calendar year		PAN mobility device**
Occasional/Ad Hoc		5 working days or less per month	No presence required	6 times per calendar year	Agreement is not required. Approval from Div Head is required	Vasco token, NU Polycom and DNBL from a private device
Regular		Up to 6 calendar months.	Minimum of 2 full day presence per week	Can be renewed	Written agreement	PAN mobility device**
Emergency	Formal order or the Division Head request	Accordance with the order			Agreement is not required	Vasco token, NU Polycom and DNBL from a private device

* Minimum CIS requirement in order that an employee will be approved to telework.
** NR laptops are an exception to perform duties when decided by the Division Head/equivalent authority. NU is the norm as the main operating network when working from home.

CHAPTER 3 - TELEWORKING AGREEMENT

3-1. **Teleworking Agreement.** An agreement establishing the duration, location, termination, type of teleworking and security arrangements, as well as the minimum required presence in the office. The teleworking agreement will be signed between the workers, their Division Head/equivalent authority and NCISG J1/NSB S1. A template of the teleworking agreement can be found at Annex A.

3-2. **The teleworking agreement shall, as minimum, stipulate:**

a. The worker's teleworking location.

b. The planned days available on the premises of the Organization.

c. The teleworking hours.

d. The equipment/supplies available to the staff.

e. The arrangements for communication and information management.

f. The arrangements for contacting the teleworker at his/her ADL.

g. The start and end dates of the agreement.

h. The security agreement covering work within non-controlled environments.

3-3. Besides this, the teleworker and their supervisor shall develop a SMART[2] plan of work against which progress will be monitored and output evaluated, to be included as an annex in the teleworking agreement.

a. A summary of specific work deliverables to be carried out.

b. A measurable output of the tasks involved and any priorities.

c. The feasibility of the duties away from the work environment.

d. The timeframe for completion of the tasks.

e. A realistic comparison between NCISG HQ or NSB HQ delivery of tasks.

f. Due to security and budget constraints, the provision of necessary equipment will be limited to available resources. Communications and sharing of sensitive and classified documents and work must be done through a secure platform.

3-4. The teleworking agreement is to be filled in and signed digitally as soon as SHAPE enables this capability within the Human Resources Data Services (HRDS) Self Service Portal.

---

[2] Specific, Measurable, Attainable, Relevant, Timely

CHAPTER 4 - RESPONSIBILITIES OF THE TELEWORKER

4-1. **Reachability.** The teleworker will be available during their Teleworking Agreement documented working hours. For security of information reasons, if the teleworker has a NATO phone or another NATO devices, it will be the principal way of contacting them. Moreover, they must be within recall distance of the HQ and be able to be present within a maximum time of 2 hours or as decided by the Division Head.

4-2. **CIS.** The teleworker is to use NATO CIS whenever possible (e.g. official laptops, phones etc.). Due to security, the provision of necessary equipment may be limited to available resources and therefore, in this case, private CIS may be used, each staff member can utilize their private CIS equipment if there has been no NATO provided equipment. More detailed information regarding the use of private CIS when teleworking is at Annex B.

4-3. The teleworker is to remain accountable, at all times, for the proper use of CIS equipment made available to them. The use of the NATO authorised CIS shall be done in accordance with the SECOPS delivered with it.

4-4. **NATO Information.** As directed by References D and F, only open source and public information, or NATO information specifically approved for disclosure to the public, can be posted on web pages and shall be subject to the integrity requirements of the originator(s) of the information.

4-5. **NATO Unclassified (NU) Information.** NATO UNCLASSIFIED (NU) information shall only be used for NATO official purposes. Practical guidance for the handling of NU information when working from home is provided within Annex B. The deliberate downgrading of NATO Classified Information to NU that circumvents NATO Security Policy to permit the use of such material by the teleworker, whether by hard copy or by transmission over any CIS equipment, is a security violation that could lead to unauthorised disclosure and possible investigation upon recognised compromise of information.

4-6. **Information classified higher than NU.** NATO Classified Information graded NATO RESTRICTED (NR) is to be protected by means of approved security mechanisms if working from an ADL. For NATO Classified Information up to and including NATO RESTRICTED (NR), the security requirements, directed in Reference D and outlined within Annex B, are to be applied. NR material must not be sent over non-authorised and non-accredited CIS.

4-7. **NATO Regulations.** The teleworker remains subject to all NATO regulations, and is to take special care to those regarding the use of NATO information and classified information, as well as the Data Protection Guidance.

4-8. **CIS Security.** When non-classified NATO information is stored, processed or transmitted electromagnetically, security measures are required to ensure its integrity and availability and also, in the case of NATO classified information, its confidentiality. CIS security requirements, outlined in Annex B, must be applied during teleworking.

4-9. **Home insurance.** The teleworker is to comply with home insurance regulations required in the HN, as well as to ensure that their home electrical installation is in compliance with HN regulations on health and safety.

4-10. **Confidentiality of Information.** Teleworkers are responsible to establish the sensitivity and safeguard the confidentiality of the information they handle while teleworking.

4-11. **Health and Safety.**

a. The worker is responsible for ensuring that a suitable workspace at the teleworking location meets standard health and safety criteria. The worker will carefully read guidelines in Annex F.

4-12. **Equipment.**

a. All computer for teleworking purposes is and shall remain the property of the providing NATO Body.

b. NCISG shall not reimburse the cost for the use of peripherals belonging to the teleworker (e.g. printers, cartridges), including costs relating to the use of the worker's own internet supplier.

c. The teleworker shall ensure that CIS equipment made available to them by NCISG shall only be used for business purposes.

d. The teleworker will provide for herself/himself appropriate ergonometric office furniture (office chair, desk, desk lamp, headphones).

4-13. **Internet connection.** Teleworker is responsible for procuring and ensuring at their own cost a secure and reliable network connection, which will allow him/her to effectively fulfil his/her duties.

4-14. **Reporting.** NATO International Civilians (NICs), Consultants, Contractors and Temporary Civilians are to report the teleworking hours as part of the monthly attendance report indicating the exact teleworking days according to the attendance report instructions.

CHAPTER 5 - RESPONSIBILITIES OF NCISG

NCISG is to maximize the usage of the NU whenever the classification permits. The NU (u000 domain) is the primary network for NCISG when Teleworking from home. Therefore, in order to avoid the risk that teleworkers will feel isolated, information shall be made available on the NU for teleworkers.

5-1. **Training.** NCISG is to provide information to teleworkers on data protection, ergonomics, security, use of IT equipment and precautions to be taken against damage and theft related to teleworking. Training will be done and tailored at NCISG HQ/ NSB level.

5-2. **Work equipment**. NCISG is to arrange for (i.e. provide, install, maintain and dispose) the NATO CIS equipment for teleworking, unless the teleworker uses their own, as well as provide appropriate technical support for NATO equipment and general support in terms of security. NCISG will not provide appropriate ergonometric office furniture (office chair, desk, desk lamp, headphones).

5-3. **Implementation of the Directive.** NCISG Division Heads, through CG is responsible for monitoring the correct implementation of this directive and avoiding any situation of unequal treatment.

5-4. **Telework related accidents.** Within the context of teleworking, an accident occurring at the ADL and during teleworking hours, and for which the teleworker provides proof that the accident occurred as a result of or in connection with their duties, shall be considered as a work accident.

5-5. **Data Management and Reporting.** NCISG J1 to coordinate with SHAPE J1 to implement the capability to record, and approve the Teleworking Agreements within the Automated Personnel Management System and support the reporting for authorised personnel within NCISG J1 in order to be able to retrieve statistical information about past and planned teleworking agreements. The exact reporting requirements are to be submitted as standard Human Resources Data Services (HRDS) reporting support requests for implementation within the HRDS tools.

ANNEX A TO
NCISGD 025-003
DATED MAR 22

TELEWORKING AGREEMENT – TEMPLATE

1. This Agreement, the Teleworking Agreement, is effective from DD/MMM/YYYY until DD/MMM/YYYY is between .....,[3] (the NCISG Teleworker) and NCISG.

2. The parties, intending to be legally bound and agree as follows:

3. **Scope of Agreement.** NCISG personnel (the 'Teleworker') agrees that teleworking is voluntary and may be terminated at any time, by either the Teleworker or NCISG, with or without cause. The Teleworker acknowledges that, if teleworking is part of the initial job description, termination of teleworking without cause may lead to administrative sanctions and even termination of the employment.

4. Other than those duties and obligations expressly imposed on the Teleworker under this agreement, the Teleworker's duties, obligations, responsibilities and conditions of employment with NCISG remain unchanged.

5. **Term of Agreement.** This Agreement shall become effective as of the date written above, and shall remain in full force and effect, unless the Agreement is terminated or unless the Teleworker contract is terminated.

6. **Type of Agreement.** This Agreement is to regulate .....[4] teleworking.

7. **Termination of Agreement.** Teleworker's participation as a teleworker is available only as long as NCISG permits, in its sole discretion. NCISG may terminate Member's participation as a teleworker, with or without cause, upon notice thereof, in writing. NCISG will not be held responsible costs, damages or losses caused by the end of teleworking. This writing is not a contract of employment and may not be construed as one.

8. **Overtime Work Compensation and Benefits.** The Teleworker agrees to obtain advance supervisory approval before performing overtime work and before taking leave. Working overtime without such approval may results in termination of the teleworking privilege and/or other appropriate action, including disciplinary action. Teleworker's compensation and benefits shall be the same for a teleworker as if employed on normal workplace.

9. **Evaluation.** The Teleworker shall be evaluated in the same manner as other NCISG Teleworkers in their classification.

10. **Provision of "Designated Remote Workspace".** The Teleworker shall identify a home location, hereafter referred to as "Workspace". This Workspace should be free of hazards to the Teleworker. If the Teleworker is injured while working in the Workspace, the Teleworker must immediately inform their direct supervisor. By signing this Agreement, the

[3] Insert name of the NCISG Teleworker.
[4] Specify long term, short term, ad hoc/occasional, regular, emergency.

Teleworker acknowledges they have complied with this paragraph and prepared a designated remote workspace.

11. **Workers' Injuries Compensation.** For NATO civilian employees, NCISG may be responsible for work-related injuries as required by NATO regulations. Any claims will be handled according to the normal NATO procedures for work-related accident claims. The military personnel will follow national procedures.

12. **Workers' Accessibility.** The Teleworker agrees to be reachable during their working hours. The Teleworker must provide a contact telephone number and email address at which they may be reached immediately. For security of information reasons, if the Teleworker has a NATO phone or other NATO device, it will be the principal way of contacting them.

13. **Access to Materials and Protected Information.** Teleworker must follow all NATO rules and regulations, as well as NCISG's policies to protect the security of NATO information. Teleworkers are responsible for maintaining the security and confidentiality of all NATO information in their possession. Failure to follow the rules, regulations and policies is grounds for disciplinary action and immediately revocation of teleworking privileges.

14. **Work Schedule.** The Teleworker agrees that the Teleworker's work schedule will be as designated in the attached Teleworking Assignment. If no special agreement is reached, the normal working hours in accordance with ND 040-010, NCISG Headquarters Working Hours, dated 31 August 2016, will apply. Any changes to the Teleworker's Work Schedule must be agreed by the Teleworker's supervisor in advance. The Teleworker agrees to maintain contact with the office as specified by the supervisor and to provide any supporting documentation for hours worked to the Teleworker's supervisor.

15. **Working Hours Supervision.** NCISG may supervise the teleworker, respecting the Teleworker's privacy and in a proportional manner. The Teleworker agrees that they may be contacted by their supervisor at a phone number so designated in the Teleworking Agreement during the scheduled working hours.

16. **Appropriate Use of NATO Provided Resources.** Teleworkers use of NATO provided resources such as accounts, equipment, software and Internet connectivity is subject to all applicable NATO Regulations, the NCPR, the NATO Code of Conduct and the Standards of Conduct (AD 040-007). Teleworkers agree to conduct all due diligences to protect NATO information, to report any breaches and incidents.

17. **The Use of Private CIS for Teleworking.** The teleworker is to use NATO CIS whenever possible (e.g. official laptops, phones etc.) due to security and budget reasons, the provision of necessary equipment is limited to available resources. During the teleworking period, the teleworker remains subject to all relevant NATO applicable regulations. More detailed information regarding the use of private CIS during the teleworking activities is mentioned in Annex B.

18. The Teleworker confirms that she/he understands that NCISG has no intent to procure and/or to financially intervene in the provision of any ergonomically adapted equipment at the Teleworker's ADL. Therefore she/he recognizes to own or will provide for herself/himself appropriate ergonometric office furniture (office chair, desk, desk lamp,

headphones). The Teleworker confirms that she/he is aware that the purchase of any furniture will not be subject to reimbursement. The Teleworker confirms that she/he cannot claim compensation for damage of health due to the lack of appropriate office furniture at the ADL.

19. The Teleworker remains obligated to comply with all of NATO and NCISG policies, rules, practices, instructions and with this Agreement. The Teleworker understands that violation of any of the above may result in preclusion from teleworking and appropriate disciplinary action.

20. The Teleworker is to comply with the minimum set of CIS requirements listed on table 2-6 for the chosen type of teleworking.

21. **Teleworker Telework Information** *(to be filled out by the Teleworker prior to signature of the Teleworking Agreement)*

Teleworker Name:	
Job Title:	
Department:	
Supervisor:	
Arrangement requested by:	☐ **Member** ☐ **Employer**
Teleworker Telephone Number:	
Teleworker Email Address:	
Location where telework will be performed:	
Telework arrangement effective dates:	

22. **Work Schedule and Location** *(to be agreed upon by the Division Head/equivalent authority and Teleworker. A copy of the weekly schedule shall be sent to both the branch/division and J1/S1, together with the Member's attendance report).*

☐ In accordance with ND 040-010

Or

Day of Week	Work Hours	Work Location
Monday		
Tuesday		
Wednesday		
Thursday		
Friday		
Saturday		
Sunday		

23. **Equipment** *(to be filled out by NCISG/NSB and the Member prior to signature of the Teleworking Agreement)*

Equipment	**Provided by**	**Responsible for loss or damage. Unless otherwise explicitly stated in writing, the teleworker is always responsible for his privately-owned or NATO-provided means.**

24. **Additional details** *(to be filled out by the Member prior to signature of the Teleworking Agreement)*

Policies, Procedure and Briefings Acknowledgement	**Teleworker's Signature**
I have read and understand NCISG's Teleworking Policy and Process.	
I have read and understand the NCPR, NATO Code of Conduct and ACO Standards of Conduct.	
I have read table 2-6 and confirm to meet with the minimum CIS requirements for the chosen type of teleworking.	
I have read and understand all the relevant and applicable NATO regulations regarding security, handling of NATO information, ACO Data Protection, etc. as determined by my Division Head/equivalent authority.	
I have read and understand the consequences of my failure to comply with the present Teleworking Agreement or any other NATO Rules and Regulations.	
I have been briefed by my Division Head/equivalent authority or their designed alternate regarding Host Nation Health and Safety regulations.	

NCISGD 025-003

I have read and understand this Agreement, discussed it with my supervisor and accept its conditions.

Teleworker:		Date:	
Division Head/equivalent authority:		Date:	
NCISG J1/NSB S1:		Date:	

NCISGD 025-003

ANNEX B TO
NCISGD 025-003
DATED MAR 22

GUIDANCE ON THE SECURITY OF NATO INFORMATION WHEN TELEWORKING

1. **Working at home with NATO UNCLASSIFIED whilst Teleworking.** When a worker has agreed to work from home, the following security measures are to be applied to protect NATO UNCLASSIFIED (NU) information:

a. Recognise the sensitivity of information and respect the marking/ classification of data in accordance with its sensitivity. Do not deliberately downgrade information (e.g. public information) to utilise non-protected teleworking or homeworking technology environments.

b. All documents are to be protected, during periods of teleworking, from anyone without a 'Need To Know', including family members.

c. When working with hard copy NU documents, do not dispose of them in any form of bin, bring them back to work or destroy them by means of burning or shredding.

d. Do not discuss information higher than NU over public means (e.g. phones).

e. For teleworking activity, use NATO or NATO approved CIS whenever possible (e. g. official laptops, phones, etc.).

f. The development and use of an "ACO NU PAN Mobility solution" was approved to support teleworking at NATO Unclassified. All NCISG Divisions are informed about the NU PAN solution (Reference I) including the specific Security Instructions to be followed[5] in addition to SecOps.

g. NU information is not to be processed on home PCs with a personal account. Only open source and public information, or NATO information specifically approved for disclosure to the public with all NATO markings removed, can be processed.

h. Only open source and public information, or NATO information specifically approved for disclosure to the public, may be posted on publicly accessible bulletin boards or web pages.

i. Do not use public cloud storage or public cloud platforms to collaborate with colleagues or to store NU (or higher) information.

j. The use of public/online meeting technology for NU information is permitted, on the condition that there is no online storage of information.

k. The teleworker is to ensure that their private CIS is safeguarded with up-to-date protection measures, malware protected, and, in case of questions, is to contact NCISG J2/6.

[5] For further details, see Reference I or its latest update.

l. Update CIS as recommended, from recommended sources (e. g. Microsoft, Adobe etc.) and maintain Anti-Malware and other security tools. It is also highly recommended to use additional tools like AdBlockers, browsing controls, privacy protecting search engines to protect teleworking efforts.

2. **Working at home with NATO RESTRICTED.** When COS NCISG has authorised[6] Teleworking with NATO RESTRICTED (NR) information, the following mitigation measures are to be applied:

a. **General**

(1) NCISG staff members can be authorised to carry paper copies of documents classified up to and including NR, or NCISG authorised CIS, granting protected access to NR information between HQ NCISG and their residence, and to store those documents at their residence:

(2) NR information shall be protected from anyone not authorised to access it, including family members; this includes prevention from overlooking.

(3) Authorisation for the removal of NR material for homeworking shall only be provided by COS, who as the ACO NCISG Delegated Authority may, on a case by cases basis, grant such approval through clear instructions that are time-bound and specific to the prevailing circumstances.

(4) It is to be noted that when so authorised by COS, such authority shall require Division Heads to assess and manage the requirement for Teleworking with NR within their Teams. COS authority will not provide blanket approval for all personnel to take NR information home with them irrespective of need, without the minimum control measures being applied.

b. **Electronic format**.

(1) Where NCISG COS has specifically authorised the deployment of an "ACO NR AIS Mobility solution" (Reference J) that allows use of NR laptops in support of existing C2 capabilities, they may be used accordingly by personnel; however, specific Security Instructions are to be understood and applied by the user[7].

(2) NR information, at the ADL, may only be processed on NR accredited/certified mobile workstations. As a consequence, NR information, utilised for Teleworking, will be either in hard copy or in electronic format. In case of the latter, it will be protected by the NATO RESTRICTED laptop, as part of the ACO NR AIS Mobility solution.

c. **Hard Copy Material**

(1) Only those who have already been authorised to remove NATO Classified Information for working at home may do so (e. g. NCISG Command Group). The removal of NATO Classified Information, including NATO

[6] For example, as directed within a COS order or initiation of the NCISG Business Continuity Plan, which confirms the requirement to telework with NR information.

[7] See Reference J or subsequent latest update for further details.

RESTRICTED, from NATO premises by anyone other than those already permitted to do so for the purpose of working at home, is strictly prohibited.

(2) Personnel shall carry NR documents in a sealed envelope bearing no external markings. Documents shall be hand-carried only by staff members categorised in paragraph 2. A. (1).

(3) Do not work on NR documents in a public place.

(4) Do not print any hard copies on a home printer or copier.

(5) When you are not working on the NR document, store it in a bag, drawer, safe or locked room.

(6) Do not dispose of NR documents in any form of bin; bring them back to work in order to destroy them or, failing this, burn them in a user-controlled manner.

(7) A register of all NR documents removed from the HQ is to be kept by the respective Branch or Division. This list is to include who has removed the document and to what postal address.

3. **Teleworking with documents classified NATO CONFIDENTIAL or above is NOT permitted over the NU, NR or the Internet both in digital and paper form.**

NCISGD 025-003

ANNEX C TO
NCISGD 025-003
DATED MAR 22

NU PORTAL PROCEDURES

Overarching principles

1. Access to the DNBL NU Portal is granted to NCISG staff from any device, NATO CIS and private after submission the request to the DNBL Functional Administrators.

2. Information on the DNBL NU Portal is structured in accordance with the NCISG organisational structure down to Command Group, J1, J2/6, J3, J4, J5, J7, J8, 1NSB, 2NSB, 3NSB.

3. Documents shall NOT contain any information higher than NU. As documents on the NU Portal are accessible by all staff with authorised access, uploading documents is limited to those stemming from:

   a. Public EDMS libraries, provided there is a need-to-know for teleworking staff.

   b. NU taskers, with the exception of close hold taskers.

Roles and responsibilities

4. NCISG CG Staff and Workflow Management Office (SWMO) is to:

   a. Administer the NU Portal as a collaborative working environment in accordance with SecOps and the NCISG organisational structure.

   b. Monitor that no sensitive information or information higher than NU is made available, as outlined in paragraph 3 above.

   c. Provide training to Divisional Security Officers (DSOs) and IKM Support Officers (IKMSOs).

5. The need for teleworkers to contribute to a certain product may require the transfer of documents to the NU Portal. Thus, the tasking authority (e.g. EXO, Action Officer) is to create a new item on the NIP Information Transfer list, comprising with the following information:

   a. Name of Task.

   b. TT+ reference (if associated to a TT+ tasker).

   c. Hyperlink to documents for transfer.

   d. Target document library on NU portal.

   e. Acknowledgment that all documents are NU.

   f. Data required.

6. When multiple documents are transferred in relation to a task:

a. It is necessary to provide clear instructions stating that the product is to be developed or supported on the NU Portal. Also, amend (or ask SWMO to amend if CG related) the tasker instructions in TT+ accordingly.

b. It is recommended to use the appropriate file naming in order to structure the files. As an example, in the context of a Tasker, the Action Officer should name the files to mirror the category in the tasker:

(1) NCISG-XXXX_00_Div_document title for Tasker instructions

(2) NCISG-XXXX_01_Div_document title for CG Point Paper

(3) NCISG-XXXX_02_Div_document title for Product

(4) NCISG-XXXX_03_Div_document title for References

(5) NCISG-XXXX_04_Div_document title for References not for CG

where: XXXX – Tasker Tracker Plus number.

7. Divisional J2/6 Security Officer (DSO), IKM Officer (IKMO) and NCISG Registry. Only DSO, IKMO and NCISG Registry are authorised to move files in accordance with existing policies and procedures. In order to balance the lack of availability of staff during periods of reduced manning, DSO, IKMO and NCISG Registry are to mutually support each other. Their role is therefore expanded to monitoring the NIP Information Transfer list and to ensuring all requests are completed irrespective of their position in the organisational structure. As a minimum, they are to review the list for open requests 3 times per day when they are in the office.

8. Documents transferred for informational or referencing purposes should be copied to the NU Portal, whereas documents required for collaborative work by staff members within and outside NCISG are to be moved in order to avoid duplication of information between domains as well as to provide visibility to contributions from other staff departments and members. Collaborative working documents taken from TT+ are to be checked out by the action officer until the work on the NU side is complete. Alternatively, the EXO/ tasking authority/ Action Officer may decide to make the document available in a non-editable format and for comments to be delivered by means of a Comments Matrix.

9. Teleworking staff are to monitor their PAN mailbox and to complete all tasks as directed by the Action Officer. Once a sub-task is completed:

a. Documents are to be saved or new documents are to be uploaded on the NU Portal in accordance with the naming convention.

b. Feedback is to be provided to the Action Officer and their acting EXO.

When products are finalised, the Action Officer can mail the packaged to their NS account (xxx.xxxx@ns.ncisg.nato.int) and save them to the correct document library or merge any changes into TT+ and check the file(s) in.

ANNEX D TO
NCISGD 025-003
DATED MAR 22

BEST TELEWORKING PRACTICES

1. Best practices include the following:

a. Office Phone Forwarding. All personnel should forward their office phones to a phone that will be monitored during remote work periods. Forwarding codes are below:

(1) Activate Call Forwarding: dial *60 – then dial 0 + (Tele-Working (TW) phone number) when prompted. Dialling prefix 0 is commercial within Belgium, 00xx – commercial outside of Belgium.

(2) Deactivate Call Forwarding: dial *64

b. Email Auto-Reply (Out of Office). All personnel are required to activate Email Auto-Reply (Out of Office) for NS email accounts when working remotely. Replies must include detailed information where to send relevant information or how to contact the addressee (phone # and monitored email) to address urgent inquiries (within one working day).

c. Email Signature Blocks. All personnel must ensure that information provided within their email signature blocks enables internal and external audiences to contact them using appropriate means. This may necessitate different signature blocks for internal and external audiences. If phones are not forwarded, then signatures blocks should include a private telephone number that is monitored while working remotely. If individuals cannot access their NATO email accounts, then signature blocks should include a functional mailbox or distribution group address.

d. Establish Structure and Framework for Communication within Teams. First line supervisors should arrange times for subordinates to contact them by phone (not email or chat) daily. Teams should arrange at least weekly teleconferences or conference calls to rapidly disseminate common information and maintain team integrity. Leaders should ensure that they have commonly available means of video teleconferencing (and that subordinates know which tools leaders use).

e. Establish Structure at the Remote Work Location. Working at home is normally difficult, because all family member are working or attending school remotely. Personal CIS is often utilised by other family members, and typically quiet workspaces may be occupied by them. Whenever possible, find a place that you can work without distractions, but also consider the needs of other family members. Balance is essential.

f. Know when to step away from your workspace. Everyone needs a break from screens at some point. Take regular breaks and exercise.

g. Maintain your calendar. Ensure you maintain your work calendar so people can contact you when needed. Skype Business is an exceptional tool for notifying team members when you are in the office.

NCISGD 025-003

h. Shared mailboxes on classified networks and distribution groups for unclassified networks. Both shared mailboxes and distribution groups provide a means of rapidly sharing information among a distributed workforce, but require leadership involvement in creating business rules that ensure accounts are checked regularly, information is processed appropriately, and action is taken in appropriate time. Two common problems are multiple people working on the same issue or no one working on an issue because they think someone else will do it. Regular communication is essential to reduce waste effort.

NCISGD 025-003

ANNEX E TO
NCISGD 025-003
DATED MAR 22

REFERENCES

A. ND 040-010, NCISG Headquarters Working Hours, dated 31 August 2016.
B. NATO Civilian Personnel Regulations (NCPR), dated November 2020.
C. JCB-D(2017)0001, NATO Joint Consultative Board, Teleworking, dated 17 July 2017.
D. AD 070-001, ACO Security Directive date 28 January 2019.
E. AD 070-005, ACO Communication and Information Systems (CIS) Security Directive, dated 28 January 2019
F. AC/35-D/2002, Directive on Security of Information.
G. AD 045-001, ACO Military Personnel – Manpower, Management and Administration for Peacetime Establishment Structures, dated 14 September 2020.
H. AD 080-116, ACO Business Continuity policy and planning, dated October 2020.
I. SH/CYBER, J6 Cy/SPP/131/20-6725, Extension of the Interim Approval to Operate for ACO NU AIS Mobility Solution to January 2021, dated 14 September 2020.
J. SH/CYBER J6 Cy/SPP/132/20-6714, Extension of the Interim Approval to Operate for ACO NR AIS Mobility Solution to January 2021, dated 14 September 2020.
K. AD 015-026, ACO Data Protection Policy, dated 17 February 2020.
L. SH 040-010, Teleworking Policy, dated 15 February 2021.
M. AD 070-007, ACO Directive, Standards of Conduct, 14 April 2020.

ANNEX F TO
NCISG/CG/SWMO/22-TT
4186 No.DIR 025-003
DATED MAR 22

HEALTH AND SAFETY GUIDELINES ON TELEWORKING

1-1. **Work environment at home.**

An appropriate work environment at home should include:

a. A room (ideally), and, if this is not possible, at least a space where the teleworker can work.

(1) It allows the teleworker to be acoustically and visually isolated, facilitating concentration and minimizing distractions.

(2) It contributes to maintaining a boundary between work and domestic life. It is a symbolic way of establishing a divide between these two spheres: getting out of the room means leaving work.

b. Adequate temperature, humidity and ventilation. Adequate lighting (including daylight) to perform tasks efficiently, accurately and in a healthy way.

c. Adequate internet connection and telephone lines (if necessary).

d. Regular checks for defects in equipment and electrical wiring.

1-2. **Display Screen Equipment (DSE) and workstation**

a. Teleworking is also associated with ergonomic risks. Working with DSE, an inadequate workstation and sedentary work are related to, among other issues, eye fatigue; musculoskeletal pain and disorders; stress; mental and cognitive workload; and the health effects related to a lack of exercise or sedentary work (i.e. obesity, type II diabetes, cardiovascular pathologies, etc).

1-3. **Equipment and environment conditions**

NCISG will not cover any expenses related to the adaptation of the home workplace. Listed below are recommendations provided for the teleworker who is responsible for deciding on the need to adjust the workplace.

a. Ergonomic work furniture (adjustable, adequate for different tasks) that helps teleworkers to maintain a comfortable, neutral body posture with joints naturally aligned, and reduce stress and strain on the muscles, tendons and skeletal system.

b. Adequate layout of the IT equipment components on the work surface in order to ensure a comfortable working position.

c. Sufficient space at the workstation, to allow the teleworker to have a comfortable position, change their position and move.

d. Adequate lighting, thermal comfort and a low noise level.

1-4. **Relationship with supervisor(s) and co-workers**

a. Duties, expectations and deadlines should be clearly outlined and agreed upon by both the supervisor and the teleworker.

b. Teleworkers are encouraged to use communication tools to inform managers/co-workers when they are 'busy', 'available', 'not to be disturbed', i.e. 'busy' when they need to concentrate on certain tasks, 'available' when they can be contacted, etc.

c. Managers will establish the hours during which they may contact with teleworkers. The Teleworker should update his/her calendars and include the hour of lunch when lunch is intended to be taken.

1-5. **Tips for balancing work and private life**

a. The main sources of stress for teleworkers include long working hours; intensive and flexible work; work organization; isolation; and the blurring of boundaries between paid work and private life.

b. Start and end the day with a routine or daily ritual (e.g. get dressed in the morning, go for a walk or any other dynamic activity – without a screen) and try to begin and finish at the same time every day.

c. Vary work tasks to avoid monotony.

d. Plan the working day and stick to it, so as to control working hours (thus avoiding overwork or continuous work).

e. Disconnect by putting away a laptop computer or switching off the (business) phone.

f. Plan and take regular and short breaks and a lunch break.

g. Have a specific room/space in which to work so that when this room is left, work is over.

h. Establish boundaries around work hours with partners, children and/or housemates.

1-6. **Tips to prevent the feeling of being isolated**

a. Isolation due to teleworking can have potential negative effects on the occupational health and well-being of teleworkers; that is why it is so important

to ensure good communication between the teleworker and the employer or co-workers.

(1) Provision of communication tools by the employer (emails, chats, shared documents, video conferencing, collaborative work tools, shared agenda) and their related support is desirable.

(2) Teleworkers use the communication tools that have been put in place by the employer to stay informed about the latest developments with work, the team and the organization.

(3) Teleworkers schedule regular meetings and catch up with the manager, team and co-workers to help maintain ongoing contacts and foster positive working relationships.

(4) Informal contact is maintained by getting together online (virtual coffee breaks, discussion forums/chats, etc.).

(5) Managers keep in touch with lone workers and ensure regular contact to make sure that they are healthy and safe (recognize signs of stress).

(6) Teleworkers establish a routine for contact with the supervisor or co-workers

(7) Employer "hot line – trust person" available for the personnel to call when feeling depressed, isolated.

b. Examples of stretching exercises that can be performed at regular intervals throughout the day:

(1) Lift your arms above your head and make circles with your arms.

(2) Shrug your shoulders and roll them backwards and forwards a few times.

(3) Roll your neck gently from left to right, focusing on tight spots.

(4) Roll your ankles, point your toes and flex your feet.

(5) Stretch your hip flexors by pointing one knee at the floor and pushing your hips forward.

(6) Lean back in the chair and push you upper arms back onto the chair to stretch your chest and shoulders.

(7) Clasp your hands behind your chair and stretch your shoulders backward.

c. Examples of sitting exercises to keep moving and active throughout the workday:

(1) Squeeze your buttocks for 5-10 seconds.

(2) Use a hand gripper to give your hands and forearms a workout.

(3) Do bicep curls with a heavy stapler or full water bottle.

(4) Swivel in your chair for an ab workout.

(5) Do leg raises under your desk.

(6) Squat over your chair for 15-30 seconds.

(7) Raise yourself above your chair using your arms.

d. Examples of exercises that can be added to your work routine:

(1) Eat lunch away from your desk.

(2) Stretch at your desk every 30 minutes.

(3) Stand and take a break from your computer every 30 minutes.

(4) Add a minimum of 10 minutes of moderate or vigorous intensity aerobic exercise to your day, which is enough to get the heart pumping and burn calories.

(5) Add more short breaks or micro breaks to your work day.