UNIWERSYTET WARSZAWSKI | MONITOR UNIWERSYTETU WARSZAWSKIEGO

Item 312

ORDINANCE No. 127
OF THE RECTOR OF THE UNIVERSITY OF WARSAW

dated 5 July 2023

on the principles of performing occasional remote work at the University of Warsaw

Pursuant to Article 23, section 2, point 2 of the Act of 20 July 2018 – the Law on Higher Education and Science (consolidated text: Journal of Laws of 2023, item 742, as amended) and § 36, section 1 of the Statute of the University of Warsaw (UW Monitor of 2019, item 190, as amended), hereinafter referred to as the "Statute", it is hereby ordered as follows:

§ 1

1. The Ordinance lays down:

1) the principles of performing occasional remote work at the University of Warsaw;
2) model documents regarding the performance of occasional remote work at the University of Warsaw;
3) the risk assessment sheet for remote work together with the rules of safe and hygienic remote work performance;
4) the personal data protection guidelines together with information security and protection requirements for remote work.

2. Whenever the Ordinance refers to:

1) the organisational unit of the University of Warsaw – it shall be understood as the organisational unit of the University referred to in § 11, section 1, points 1-6 of the Statute;
2) the employer – it shall be understood as the University of Warsaw;
3) the employee – it shall be understood as an academic or an employee who is not an academic, but has an employment relationship with the employer;
4) the head of an organisational unit – it shall be understood as the head of an organisational unit of the University;
5) the direct superior – it shall be understood as the head of an organisational unit of the University or the head of an internal organisational unit, if provided for by the regulations of such organisational unit of the University;
6) remote work – it shall be understood as work performed partially or in whole in a place indicated by the employee and in each instance agreed with the employer, including but not limited to the employee's home address, in particular using the means of direct distance communication.

7) occasional remote work – it shall be understood as remote work performed occasionally upon the application of the employee, filed electronically, for up to 24 days per calendar year, as referred to in Article 67^{33} of the Act of 26 June 1974 of the Labour Code (consolidated text: Journal of Laws of 2022, item 1510, as amended).

§ 2

1. Occasional remote work may be performed by academics and employees who are not academics, subject to sections 2 and 3, if the following conditions regarding the work organisation and nature of work for a specific job position are cumulatively met:

1) work may be performed outside the employer's premises, on the territory of Poland;
2) the nature and scope of the duties performed by the employee or work organisation and the characteristics of the tasks carried out by the organisational unit of the University, in which the employee performs their duties, do not require the direct presence of the employee on the employer's premises in order for the employee to perform their work;
3) the results of the work can be submitted to the direct superior by means of electronic communication and the direct superior has the ability to monitor the work performed and its results;
4) the employee uses portable work equipment to perform remote work;
5) it is possible to maintain the high quality of work, the performance of remote work does not lead to the decrease of its efficiency or deterioration of cooperation between employees;
6) remote work will be performed under conditions respecting occupational health and safety regulations, personal data protection guidelines together with information security and protection requirements.

2. Employees occupying positions in the following groups of positions are excluded from performing occasional remote work:

1) services;
2) security;
3) drivers;
4) manual workers;
5) instructors.

3. Occasional remote work does not cover:

1) particularly hazardous work;
2) work that exceeds the acceptable norms of physical elements for residential premises;
3) work with the hazardous chemical agents referred to in occupational health and safety regulations related to the presence of chemical agents in the workplace;
4) work that involves the use or release of harmful biological agents, radioactive substances, and other substances or mixtures that emit noxious odours;
5) work that produces excessively dirty substances.

§ 3

1. Occasional remote work may be performed only upon the application of the employee submitted electronically and adopted by the employer, no later than one business day before the planned day of commencing occasional remote work. In specific cases, an application may be considered if it was submitted by the employee before working hours on the day of performing remote work.

2. The application is submitted to the head of an organisational unit of the University and requires approval by the direct superior.

3. In the application for occasional remote work, the employee designates the location of work (full address).

4. The application is submitted according to the template constituting Appendix No. 1 to this Ordinance.

5. The place of performing remote work shall be agreed with the head of an organisational unit of the University.

6. The head of the organisational unit of the University shall decide whether to grant permission for performing occasional remote work.

7. The application for occasional remote work is not binding on the employer. The head of the organisational unit of the University may refuse to grant permission for occasional remote work, in particular if the conditions referred to in § 2, section 1 are not met, including if the employee's presence at the workplace is necessary due to the work organisation or the nature and characteristics of the work performed.

8. The amount of occasional remote work shall not exceed 24 days per calendar year and shall not depend on the employee's working hours (FTE), as well as on the number of hours resulting from the employee's schedule of working time on the day on which the employee performs the work. Occasional remote work is performed on full working days. Unused days are not transferred to the following year.

§ 4

1. The performance of occasional remote work is only permitted on the days when the employee performs work in accordance with the established work organisation and during the working hours established in the schedule of working time.

2. The employee performing occasional remote work shall be obliged to:

1) follow on an ongoing basis the instructions of their superiors whether issued to the employee orally, in writing or electronically;
2) remain available and ready to perform work during working hours;
3) communicate with their superiors by means of direct distance communication with regard to the rules on using a University of Warsaw e-mail account;
4) remain in regular contact with co-workers, superiors and interested parties, using available communication channels and official mail, with regard to the rules on the use of the University of Warsaw e-mail;
5) confirm their attendance at work in a manner agreed with the direct superior;
6) maintain the equipment entrusted to them and use it solely for work purposes;
7) protect entrusted hardware, software and communication equipment from damage, theft, destruction and unauthorised use;
8) comply with the employer's personal data protection obligations together with information security and protection requirements;
9) organise their workstation in such a manner as to ensure occupational health and safety conditions.

3. During the period of occasional remote work, the employee is obliged to appear at the workplace on the employer's premises when demanded by their superiors during the agreed working hours. The employee shall be notified of the date on which they are to make an appearance at the employer's premises in advance, considering the possible arrival time from the agreed remote workstation. The employer does not cover the cost of the employee's commute to work.

§ 5

1. The place of performing occasional remote work shall comply with the occupational health and safety requirements.

2. The employee organises the occasional remote workstation with regard to the ergonomic requirements.

3. Performing occasional remote work in public places is not permitted.

4. Before the employee is allowed to perform occasional remote work, they shall confirm, in a declaration submitted electronically and adopted by the employer, that they have taken note of the risk assessment and information providing the rules of safe and hygienic remote work performance and undertake to comply with them.

5. Allowing the employee to perform occasional remote work is subject to the employee submitting a declaration electronically and adopted by the employer, confirming that safe and hygienic working conditions are ensured at the remote workstation, in the work location designated by the employee and agreed with the head of the organisational unit of the University.

6. The risk assessment sheet for occasional remote work together with the rules of safe and hygienic remote work performance constitute Appendix No. 2 to this Ordinance.

7. The declarations referred to in sections 4 and 5 shall be submitted on a form constituting Appendix No. 3 to this Ordinance.

§ 6

1. The employee performing occasional remote work confirms in an electronic form and adopted by the employer that they have taken note of and are obliged to comply with the personal data protection guidelines together with information security and protection requirements for remote working defined by the employer.

2. Allowing the employee to perform occasional remote work is subject to the employee submitting a declaration in an electronic form and adopted by the employer, confirming that they have taken note of and agree to comply with the personal data protection guidelines together with information security and protection requirements for remote work.

3. Personal data protection guidelines together with information security and protection requirements for remote working constitute Appendix No. 4 to this Ordinance.

4. The declarations referred to in section 2 shall be submitted on a form constituting Appendix No. 5 to this Ordinance.

§ 7

1. The head of the organisational unit shall have the right to carry out checks on occasional remote work performed by the employee, occupational health and safety checks as well as checks on compliance with the personal data protection and information security requirements.

2. The check shall be carried out on terms agreed with the employee.

3. The head of the organisational unit of the University adapts the method of carrying out the checks to the location of the remote work and its nature. Carrying out the check shall not infringe on the privacy of the employee performing the remote work

and other persons, nor impede the use of the premises where the remote work is performed in a manner consistent with their intended use.

4. If any violations of occupational health and safety regulations or personal data protection and information security requirements are discovered, the head of the organisational unit:

1) orders the employee to remove the identified deficiencies within a specified period of time, or
2) withdraws the employee's permission to perform occasional remote work.

§ 8

The Ordinance shall enter into force on 01 September 2023.

Rector of the University of Warsaw: *A. Z. Nowak*

Appendix No. 1
to the Ordinance No. 127 of the Rector of the University of Warsaw
on the principles of performing occasional remote work
at the University of Warsaw
dated 5 July 2023

……..……..
(date)

……..……..
(name and surname of the employee)

……..….
(job title)

…….
(organisational unit of the UW)

APPLICATION FOR PERFORMING OCCASIONAL REMOTE WORK

Pursuant to Article 67[33] of the Labour Code and Ordinance No. 127 of the Rector of the University of Warsaw on the principles of performing occasional remote work at the University of Warsaw dated 5 July 2023, I am applying for a permit to perform occasional remote work in the following period:

from…… to…… .

REMOTE WORK LOCATION

Remote work will be performed:

☐ **at my place of residence:**

Address (in Poland):
postal code…….
town/city:…….
street: ……., building No. …….. flat No. …….

☐ **at another place:**

Address (in Poland):
postal code…….
town/city:…….
street: ……., building No. …….. flat No. …….

DECLARATIONS OF THE EMPLOYEE APPLYING FOR REMOTE WORK:

- I have been informed of the occupational risks attached to performing remote work and how to protect myself from any hazard that may arise;
- I have read the principles of safe and hygienic remote work performance and undertake to comply with them;
- there are safe and hygienic working conditions at the remote workstation, in the work location designated by me and agreed with the employer;
- I declare that I have read the Personal Data Protection Guidelines and the requirements for information security and protection while working remotely, and I undertake to comply with them;
- I declare that I have read the principles of performing occasional remote work specified in the Ordinance No. 127 of the Rector of the University of Warsaw on the principles of performing occasional remote work at the University of Warsaw dated 5 July 2023, and I undertake to comply with them.

……..
Employee's signature

DIRECT SUPERIOR OPINION

☐ **I approve the application** ☐ **I do not approve the application**

Date: …… ……..
signature

DECISION OF THE HEAD OF THE UW ORGANISATIONAL UNIT

☐ **I grant consent** ☐ **I do not grant consent**
to perform occasional remote work by the applicant

Date: …… ……..
signature

Appendix No. 2
to the Ordinance No. 127 of the Rector of the University of Warsaw
on the principles of performing occasional remote work
at the University of Warsaw
dated 5 July 2023

UNIVERSITY OF WARSAW

RISK ASSESSMENT SHEET

FOR REMOTE WORK

OPERATION/ACTIVITY Operating computer equipment, monitor, printer, and archiving on media while preparing necessary documentation.

DANGER: POSSIBLE DANGEROUS EVENT	**POSSIBLE RESULT OF THE EVENT**	**RESULT**	**POSSIBILITY**	**RISK**	**RISK CAN BE REDUCED BY:**	**RISK AFTER REDUCTION**
1	2	3	4	5	6	7
Nuisances specific to working on a computer	Stiffness of muscles, arms, hands, neck, back and shoulders, headache	LOW	MEDIUM	LOW	Relaxation - performing simple exercises during scheduled breaks from computer work (at least 5 minutes after each hour of work at the computer monitor - other activities).	LOW
Hitting against immovable objects (e.g., furniture) Falling on the same level (tripping, slipping)	Bumps, bruises Fracture, concussion, bruising	MEDIUM	LOW	LOW	Proper organisation of space, exercising caution Maintaining order, non-slippery floors	LOW
Excessive eyestrain	Bloodshot eyes, eyelid twitching, pinching and burning sensations, impaired visual acuity, increased squinting, decreased eye hydration, decreased vision.	MEDIUM	HIGH	MEDIUM	Adapting the computer specifications and its settings to suit the individual operator, i.e. proper contrast and lighting, right colour saturation on the computer monitor, adequate font, use of corrective glasses	LOW

Insufficient lighting of the computer workstation	as above	MEDIUM	MEDIUM	MEDIUM	Use of balanced room lighting according to Polish norms	LOW
Fire	Local or generalised burns, smoke inhalation, permanent disability or death	HIGH	LOW	LOW	Complying with principles and instructions, regular inspections of the operation of equipment and electrical installations, and providing regular training on occupational health and safety and fire safety.	LOW
Mental strain, stress, lack of direct and immediate communication when problems arise	Neurosis, myocardial infarction, stroke, nervousness, cardiovascular syncope (fainting), peptic ulcer	MEDIUM	HIGH	MEDIUM	Relaxation exercises to relieve possible tension, rest and breaks, performing work in an area that is not used by other family members.	LOW
Short circuit of the electrical installation, electric shock with voltage up to 1kV.	Indirect post-electric shock injury, local burn, death	HIGH	LOW	MEDIUM	Compliance with the principles, equipping workstations with certified devices, regular inspections and measurements of installations, and repair of equipment at an authorised service centre, if necessary.	LOW
OVERALL RISK LEVEL AFTER REDUCTION					**ACCEPTABLE**	

The assessment was developed by the Inspectorate of Occupational Safety, Health and Fire Protection of the University of Warsaw.

PRINCIPLES OF SAFE AND HYGIENIC REMOTE WORK PERFORMANCE

1. You can proceed to work remotely, having read these principles.

2. Eliminating or reducing the arduousness of computer work requires the application of a regime of working conditions in accordance with the guidelines set forth in the appendix to the Regulation of the Minister of Labour and Social Policy as of 1 December 1998 on occupational health and safety in the workplaces equipped with screen monitors (Journal of Laws of 1998, No. 148, item 973), i.e.:

1) setting the monitor screen relative to light sources should reduce glare and reflection;
2) the employee's eye distance from the monitor screen should be 400-750 mm;
3) the top edge of the monitor screen should be at eye level or 20^{0} below;
4) lighting should ensure the comfort of working with eyes;
5) setting the keyboard so that the distance between the keyboard and the front edge of the table is not less than 100mm;
6) the chair should have sufficient stability with adjustable settings;
7) the design of the table should allow convenient setting of workstation equipment elements;
8) maintain a relative humidity of not less than 40% in the room;
9) when sitting, change positions frequently to reduce muscle fatigue.

3. Prohibitions applicable with regards to the remote workstation:

1) no eating at the workstation;
2) no smoking at the workstation;
3) no unauthorised repair of computer devices, equipment and station equipment;
4) no wearing of magnetic jewellery;
5) no wet cleaning of the live computer case;
6) no using solvents to clean computers;
7) no obstructing the ventilation holes of the computer.

4. Any irregularities noted in the computer operation and its auxiliary equipment should be immediately reported to the supervisor.

5. You have to turn off the equipment and disconnect its power supply each time you finish work. If any adverse or other event that may have the characteristics of an accident occurs, you have to notify the appropriate emergency services. The direct superior should be notified immediately of the accident.

Appendix No. 3
to the Ordinance No. 127 of the Rector of the University of Warsaw
on the principles of performing occasional remote work
at the University of Warsaw
dated 5 July 2023

……..……..
(date)

……..……..
(name and surname of the employee)

……..….
(job title)

…….
(organisational unit of the UW)

DECLARATION

I declare that:

– I have been informed of the occupational risks attached to performing remote work and how to protect myself from any danger that may arise;
– I have read the principles of safe and hygienic remote work performance and undertake to comply with them;
– there are safe and hygienic working conditions at the remote workstation, in the work location designated by me and agreed with the employer;

……
Employee's signature and date

Appendix No. 4
to Ordinance No. 127 of the Rector of the University of Warsaw dated 5 July 2023
on the principles of performing occasional remote work
at the University of Warsaw

Personal data protection guidelines and information security and protection requirements for remote working

§ 1

1. The present Guidelines outline the personal data protection principles and information security and protection requirements for remote working.

2. The employer, shall provide, where appropriate, the employees performing work remotely with briefing and training in this field.

3. Information regarding training on the principles of personal data processing and information security during remote working shall be available on the website: https://odo.uw.edu.pl/szkolenia/

4. When working remotely, the employee may process personal data and other information to which they have access only for the purposes that are related to the performance of the duties entrusted to the employee.

5. During remote working, the employee shall be obliged to have due regard for the security, confidentiality and integrity of the data to which they have or shall gain access.

6. The employee shall be bound to immediately inform the Data Protection Officer, their direct superior and the IT specialist who supports the given organisational unit of the University, about any incident involving a breach of data protection and information security, including data leakage in both electronic and paper form, as well as theft or loss of equipment, which was entrusted to them.

7. Performing work remotely shall not exempt the employee from compliance with the applicable internal regulations at the University of Warsaw on personal data protection, including in particular Ordinance No. 51 of the Rector of the University of Warsaw of 15 May 2018 on the protection of personal data at the University of Warsaw (Monitor UW of 2018, item 142, as amended), constituting appendices to the Ordinance.

8. The notification of personal data breaches shall be made in accordance with the procedure set out in the Operational instructions in the event of a personal data breach at the University of Warsaw constituting Appendix No. 13 to the Personal Data Protection Policy at the University of Warsaw (Monitor UW of 2018, item 142 as amended).

§ 2
Data security and protection at the remote location

1. In the course of remote work, the employee shall:

1) agree with their household members on the rules concerning the carrying out of the work, in the case of working from home;
2) designate a workstation;
3) use automatic computer locking after a short period of inactivity (3-5 minutes) and log off from the system when leaving the workstation (even for a short while);

4) ensure that unauthorised persons (including family members) do not gain the possibility of accessing/consulting the official documents that are processed in electronic or paper form;
5) ensure the confidentiality of official conversations (including calls and online meetings);
6) ensure the supervision of documents, data carrier and other remote work equipment (e.g. laptop, tablet, phone);
7) carry and store the equipment safely.

2. When performing remote work using an Internet connection, the employee shall comply with the following recommendations:
1) in order to access the Internet during remote working, it is advisable to use cable connections or appropriately secured wireless networks;
2) to use the wireless connection that requires password authentication (at least 12 characters, including upper and lower case letters, numbers and special characters);
3) the use of public Wi-Fi networks is prohibited;
4) to restrict access to the router's administration panel to the local network only and to change the router's default password to one containing at least 12 characters.

§ 3
Work with electronic data circulation

1. Remote working is carried out through user accounts with permissions granted by the employer. The data for authentication to the employer's internal systems and services may not be communicated to third parties, and no person may log in to or use the accounts of other employees.

2. The access to the computer and other portable devices shall be secured with a strong password (recommended password length of at least 12 characters), PIN code or token.

3. The same password shall not be used for logging into multiple information systems.

4. It is forbidden to save passwords in web browsers; it is acceptable to use professional tools for password management though.

5. Computer and portable drives shall be encrypted.

6. No unlicensed software may be installed on equipment provided for remote working.

7. Antivirus software shall be used and updated in accordance with the manufacturer's recommendations. The operating system shall be kept up to date with the latest patches and fixes.

8. When connecting to the employer's network resources, the employee shall be required to use a secure connection via a VPN.

9. It is highly recommended to use two-factor authentication, wherever possible.

10. Unnecessary electronic documentation shall be permanently deleted from the hard drive, network drive or e-mail inbox, including the "recycle bin" folder.

11. The microphone and camera on the computer shall be turned off if they are not required for work at any given moment.

12. The transfer of files containing personal data and other protected information shall be carried out using tools/applications provided by the employer.

13. The employee shall be obliged to make backup copies. A backup copy shall be made on a separate secure data carrier and safely stored.

14. When performing assigned tasks, one shall avoid opening anything other than official work applications in order to reduce the risk of accidental sharing of information and personal data.

15. All problems concerning the use of IT equipment and systems shall be immediately reported to the IT staff of the respective organisational unit of the University.

§ 4
Working with hard copy documentation

1. Working on hard copy documents shall be limited to the minimum necessary.

2. The necessity to use hard copy documents outside the permanent work location shall be reported to the direct superior and shall require his/her consent. A record shall be kept of the documents made available to the employee for purposes of remote working.

3. Hard copies of official documents may only be used for the performance of official tasks.

4. It is prohibited to take photographs of the documentation or record its contents in any other way.

5. Printing of documents on private printers may only be done if it is necessary for fulfilling a particular official task.

6. Hard copy documentation shall be shall be protected against unauthorised access by third parties, including family members. Official records shall be kept in specially designated places with impeded access to third parties.

7. All the protective measures shall be taken while carrying/transporting the documents, including in opaque folders, binders, envelopes, bags, etc.

8. It is forbidden to throw the documents that contain protected/confidential information and personal data to the bin; if necessary, the documents shall be secured and destroyed in a shredder upon return to the employer's official location.

9. Official documents shall be immediately returned upon the end of the remote work.

§ 5
E-mail

1. The use of official e-mail shall be in accordance with the principles set out in Ordinance No. 279 of the Rector of the University of Warsaw of 10 December 2020 on electronic mail of the University of Warsaw (Monitor UW of 2020, item 496).

2. When it comes to official purposes, the official mailbox shall be used.

3. No private e-mail accounts shall be used for official communications (i.e. no sending of information, data or files).

4. One shall not open attachments from an unknown source.

5. Before sending an e-mail, it shall be verified that the addressee has been indicated correctly.

6. Files containing personal data, confidential information shall be encrypted prior to sending.

7. The transfer of large-sized files shall be carried out using proven solutions provided by the employer.

§ 6
Principles of videoconferencing

1. Videoconferencing shall be held using IT tools which are authorised and provided by the employer or by the entity hosting the videoconference.

2. Prior to the videoconference:

1) one shall read the terms and conditions of use or privacy policy of the programme;
2) it shall be verified if the conversations are recorded and stored;
3) it shall be checked what data permissions are being requested: contact list, location, etc;
4) applications for videoconferencing shall be downloaded from official sources;
5) care shall be taken to ensure that the area covered by the transmission guarantees the privacy of its user/participant;
6) it shall be verified that the video conferencing application ensures all the security measures required - encryption;
7) all unnecessary windows shall be shut so that other participants do not see them;
8) the microphone and camera shall be turned off when logging in to the videoconference.

3. During the videoconference:

1) the amount of personal information provided shall be reduced to a minimum;
2) links to official videoconferences shall not be shared on social media;
3) screen sharing options shall be managed;
4) official documents shall not be shared via chat, which may be public;
5) the "waiting room" feature shall be used so as to control the persons participating in the videoconference.

4. After the videoconference:

1) the microphone and camera shall be turned off;
2) It shall be ascertained that the online meeting has been ended;
3) it should be verified that the videoconferencing application is not running in the background.

§ 7
Final provisions

1. On matters not covered by these Guidelines, university regulations and provisions of generally applicable law shall apply.

2. The employee's declaration that they have read the Personal data protection guidelines together with information security and protection requirements for remote working forms an integral part of these Guidelines.

Appendix No. 5
to the Ordinance No. 127 of the Rector of the University of Warsaw
on the principles of performing occasional remote work
at the University of Warsaw
dated 5 July 2023

……..……..
(date)

……
(name and surname of the employee)

……
(job title)

……
(organisational unit of the UW)

EMPLOYEE DECLARATION
of reading the Personal Data Protection Guidelines
and information security and protection requirements when working remotely

I declare that I have read the Personal Data Protection Guidelines and the requirements for information security and protection while working remotely, and I undertake to comply with them;

…..…..……
Employee's signature and date