



Политика за допустимо използване на ресурсите на изчислителната инфраструктура към ЦВП по информатика и ИКТ

Обща политика за използване

1. Увод

1.1. Тази Политика за Допустимо Използване (ПДИ) се прилага за всички потребители на **ресурсите** на изчислителната инфраструктура към Центъра за върхови постижения по информатика и ИКТ, която се изгражда в рамките на проект BG05M2OP001-1.001-0003-C01 по оперативна програма „Наука и образование за интелигентен растеж“.

1.2. За целите на тази ПДИ, термините имат следните значения:

1.2.1. **Ресурси** са всички ИКТ функционалности, които са предоставени като част от **Инфраструктурата** и включват:

- ✓ сървъри;
- ✓ работни станции;
- ✓ високопроизводителни изчислителни карти (ускорители) инсталирани в някои от сървърите и работни станции;
- ✓ компютри за отдалечен достъп;
- ✓ дискова памет;
- ✓ локален мрежови достъп;
- ✓ глобален мрежови достъп (Интернет);
- ✓ документация и учебни материали.

1.2.2. **Доставчик на Ресурси** е административен и технически екип, упълномощен да поддържа **Ресурсите** да бъдат функционални, използваеми, в добър работен ред и да предоставя достъп до тях;

1.2.3. **Потребител** означава индивид, който е одобрен за използване на **Ресурсите**;

1.2.4. **Зловреден софтуер** означава компютърен вирус, троянски кон, червей, логическа бомба или друга зловредна програма;

1.2.5. **Проект** означава изследователска работа изпълнявана от група **Потребители**;

1.3. Целта на този документ е да дефинира правилата и терминологията управляващи допустимото използване на **Ресурси** (процесорно време, оперативна памет, лицензи, размер на данните, както и мрежовата свързаност и техническата поддръжка), включително достъп, оползотворяване и сигурност на ресурсите и данните.

- 1.4. **Доставчикът** на **Ресурси** може да направи актуализация ПДИ по всяко време, като информира за това Потребителите. Ако Потребител не приема направените промени, то може да се откаже от използването на Ресурси по всяко време.
- 1.5. Всички Потребители са длъжни да се подпишат, че са съгласни с документа Политика за Допустимо Използване (ПДИ).
- 1.6. **Потребителят** също е длъжен да следва политиките за допустимо използване на компютърните мрежи, през които осъществява достъпа до Ресурси, т.е. мрежите на БИОМ (Българска Изследователска и Образователна Мрежа), ИИКТ-БАН, БАН и политиките за допустимо използване на други организации и проекти, които посредничат за достъп до Ресурсите.

2. Общо използване

- 2.1. **Потребителят** трябва да спазва принципите, които контролират достъпа до **Ресурси** да се използва изключително само за мирни цели и етично да провежда дейностите си.
- 2.2. **Потребителят** се съгласява, че информацията събирана за неговата дейност, включително тази от регистрацията му, се използва само за административни, оперативни, счетоводни, мониторингови действия, както и за сигурност. Тази информация може да бъде предоставена чрез сигурни механизми, само за същите цели и само ако е необходима на други организации кооперирани с **Доставчика**. **Доставчикът** не дава гаранция за поддържане на конфиденциалност.
- 2.3. **Потребителят** е длъжен да информира **Доставчика** за възникнали промени в контактните си данни.
- 2.4. **Потребителят** се съгласява да използва **Ресурсите** само, за да изпълнява задачи, или да прехвърля данни, съобразно установените цели, политики и условия за използване, както те са дефинирани от **Доставчика**.
- 2.5. Правото за използване на **Ресурси** е строго персонално и не може да бъде преотстъпвано на трети страни. **Доставчикът** е упълномощен да регулира, ограничава или прекратява достъпа на **Потребителя** в рамките на неговите пълномощия и **Потребителят** е длъжен незабавно да изпълнява инструкциите на **Доставчика**. Правото за използване на **Ресурси** се прекратява, когато изтича периодът на тяхната достъпност.
- 2.6. **Потребителят** е уведомен, че използването на **Ресурси** от граждани на някои държави може да бъде ограничено от съответните Доставчици на ресурси.
- 2.7. **Потребителят** трябва да уважава всички права на собственост (които също могат да бъдат и интелектуална собственост) принадлежащи на **Доставчиците**, включително всякакви лицензи.
- 2.8. **Потребителят** трябва да спазва конфиденциалност за всякаква информация, която е получена при използването на **Ресурси**, която резонно очаква да бъде конфиденциална или чувствителна.
- 2.9. **Доставчикът** си запазва правото да управлява използването на **Ресурси**, за да осигури пълна оптимизация, дори ако това може да предизвика известни ограничения на използването от **Потребителя** или да промени самите **Ресурси**.
- 2.10. **Потребителят** е длъжен да не прехвърля данни, за които е възможно резонно да се очаква, че са конфиденциални или чувствителни, т.е. потребителски имена и пароли за ИТ инфраструктурата, без да са взети адекватни мерки за защита (криптиране).

- 2.11. Използването на **Ресурси** е на отговорност и риск на **Потребителя**. **Доставчикът** не гарантира тяхната достъпност и дали са подходящи за целта.
- 2.12. **Доставчикът** не е отговорен за никакви щети понесени от **Потребителя**.
- 2.13. **Потребителят** трябва упражнява всякакви резонни грижи за сигурност и съхранение на собствените си данни при достъпа си до **Ресурси**.

3. Недопустимо използване

- 3.1. **Потребителят** не трябва да използва **Ресурси** за недопустими цели. Недопустимите цели включват, но не са ограничени до:
 - 3.1.1. всяка дейност, която е незаконна според локалното, националното или международното законодателство;
 - 3.1.2. всеки опит за нарушение или заобикаляне на административни или защитни правила;
 - 3.1.3. всяко създаване, съхраняване или предаване на данни, които са в нарушение на авторско право или лиценз;
 - 3.1.4. всяка дейност, която целево предизвиква материални или морални щети на **Доставчика** или която довежда до загуба на оперативна ефективност или загуба или повреда на **Ресурси**;
 - 3.1.5. всяка дейност, която пречи на използването на **Ресурси** от други **Потребители**;
 - 3.1.6. всяка дейност, която компрометира личните данни на друг **Потребител**;
 - 3.1.7. всяка дейност, която може да доведе до разпространение на Зловреден Софтуер.

4. Сигурност

- 4.1. **Потребителят** е отговорен за защитата на детайлите на собствения си потребителски акаунт и средства за достъп.
- 4.2. **Потребителят** не трябва да разкрива детайлите за своя достъп до **Ресурси**.
- 4.3. **Потребителят** не трябва да използва правата за достъп до **Ресурси** на друг **Потребител**.
- 4.4. **Потребителят** е длъжен да предприеме всички резонни стъпки, необходими за защита от неправомерен достъп на компютрите, лаптопите и работните станции, от които осъществява достъпа си до **Ресурси**. Препоръчителните мерки за сигурност включват използване на парола при защита на екрана или заключване или изключване на терминалите, когато ги оставя ненаблюдавани или не се използват.
- 4.5. **Потребителят** не трябва да използва програми, които излагат на опасност функционирането на **Ресурсите**. **Доставчикът** уведомява **Потребителя**, който трябва да предприеме действия за откриването на опасността и нейното предотвратяване. Според свое резонно мнение, **Доставчикът** може да отнеме достъпа на **Потребителя** до **Ресурси**, ако е необходимо и да забрани всяка компютърна програма, която предизвиква заплахата за сигурността.
- 4.6. **Потребителят** се съгласява с всякакви специални условия, които могат да се отнасят до специфичен софтуер инсталиран на **Ресурсите**.

- 4.7. **Потребителят** е длъжен незабавно да уведоми **Доставчика**, ако разбере за неправомерно използване на потребителския си акаунт или знае или се съмнява за пробив в сигурността или нерегламентирано използване на **Ресурси**. Неспазването на това условие довежда до прекратяване на достъпа на **Потребителя** от страна на **Доставчика**.

5. Отговорности и Санкции

- 5.1. **Потребителят** е отговорен за всякакви щети заради нарушение на тази ПДИ или други политики и условия наложени от **Доставчика** и които са доведени до знанието на **Потребителя**.
- 5.2. За всяко нарушение или потенциално такова, **Потребителят** се уведомява писмено. Ако нарушението продължава и/или други нарушения са установени и/или е оправдано от сериозността на нарушението, **Доставчикът** може да отнеме правата за достъп до **Ресурси** и/или да предприеме дисциплинарни действия и/или да започне съдебни дела срещу **Потребителя**.

Политика за Специфично Използване

6. Достъп до услугите

- 6.1. Услугите инсталирани на Инфраструктурата се предоставят като споделени **Ресурси**. Достъпът до услугите не е гарантиран. За осигуряване на равномерен достъп на всички проекти се налагат специални ограничения. Всякакво използване на услуги трябва да е съобразно следващите препоръки. На **Потребители**, които системно нарушават тези препоръки ще им бъде отнеман достъпът до **Ресурси**.
- 6.2. Достъпът до Високопроизводителните сървъри се осъществява чрез **ssh** до съответните компютри или други интерфейси, които могат да са предназначени за директен достъп (Уеб портали) и всякакъв достъп до изчислителни компютри трябва да бъде през платформата за управление на задачите (batch system). Директен достъп до изчислителните компютри не е разрешен.
- 6.2.1. ssh сесиите, които са неактивни за даден период от време, автоматично се прекратяват;
- 6.2.2. тези ограничения може да се променят при необходимост от контрол на ресурсите за достъп и в съответствие с приложените стандарти за сигурност.
- 6.3. Процеси използващи значителни изчислителни ресурси или памет, не трябва да се изпълняват на споделени компютри за достъп. Такива процеси могат да се изпълняват чрез платформата за управление на задачите (batch system) или на резервиран за целта компютър за достъп. Процеси изпълняващи се на споделени компютри за достъп, които заемат значително процесорно време или памет, ще бъдат прекъсвани без уведомление.
- 6.4. Файлови системи от тип Scratch (временни) са предназначени за запис на данни за изпълнявани изчислителни задачи или се намират под активен анализ. Забранени са техники за избягване на автоматизираното почистване на такива файлови системи. Файловете на тези системи може да бъдат изтрети по всяко време и на тях не им се правят резервни копия – единствени копия на важни файлове не трябва да се съхраняват на Scratch файлова система.



- 6.5. **Потребителите** се очаква да използват ефективно **Ресурсите**, за да продължат изпълнението на изчислителни задачи на Инфраструктурата.
- 6.6. **Ресурсите** изисквани за изчислителни задачи, трябва да бъдат толкова акуратни, колкото е възможно, дори когато подобни заявки биха довели до по-дълго чакане в опашката на задачите (т.е., ако задачи изискват много голяма част от паметта на всеки изчислителен компютри, те трябва да имат зададена опция за изключително използване на паметта, дори това да доведе до по-дълго чакане в опашката).

7. Предоставяне на потребителски достъп до Ресурси

- 7.1. Всеки, който иска и има основание да стане **Потребител**, трябва да попълни и подпише следните формуляри достъпни на сайта на ЦВП по информатика и ИКТ (<http://ict.acad.bg>):
- 7.1.1. Заявка за потребителски достъп до **Ресурси**;
- 7.2. **Доставчикът** на ресурси дава или отказва достъп до **Ресурсите** в рамките на 14 - дневен период, като съобщава решението си по ел. поща.
- 7.3. Периодът на достъп до **Ресурси** за даден **Потребител** започва след подписване на две копия от тази ПИД от страна на упълномощен представител на **Доставчика** и от **Потребителя**.

Име и фамилия на
упълномощения представител
на **Доставчика** на **Ресурси**: _____

Подпис на упълномощения представител
на **Доставчика** на **Ресурси**: -----

Дата: _____

Име, презиме и фамилия на **Потребителя**: _____

Подпис на **Потребителя**: -----

Дата: _____