1. **Purpose**

   It is everyone’s responsibility to protect OVP Biotech’ intellectual, employee, customer, and partner information. The purpose of this policy is to define OVPs acceptable use of Information Technology to conduct business on company devices or network.

2. **Scope**

   This policy applies to all employees, contractors, and partners that have or require access to OVP systems or data.

3. **Responsibility**

Role	**Responsibilities**
All Employees	Responsible for taking all necessary precautions to protect OVP Biotech’ intellectual, employee, customer, and partner information and equipment

4. **Definitions**

   None

5. **Procedure**

   5.1. Use of IT Systems

   5.1.1. All data stored on OVP Biotech systems is the property of OVP Biotech. Users should be aware that the company cannot guarantee the confidentiality of information stored on any OVP system except where required to do so by local laws.

   5.1.2. OVP Biotech systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However, it must not be in any way detrimental to users own or their colleague’s productivity.

   5.1.3. Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

   5.1.4. OVP Biotech trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company’s IT systems. If employees are uncertain they should consult their manager.

   5.1.5. All laptops that have access to, or store OVP Biotech data must be encrypted to ensure unauthorized access is prevented (or at least made extremely difficult).

5.1.6. IT can monitor the use of its electronic systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any user.

5.1.7. IT reserves the right to regularly audit networks and systems to ensure compliance with this policy.

5.2. Data Security

5.2.1. If data on OVP Biotech systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information.

5.2.2. Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

5.2.3. Users must not send, upload, remove on portable media or otherwise transfer to a non-OVP Therapeutic system any information that is designated or reasonably regarded as confidential or containing personal information.

5.2.4. Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with OVP’s password complexity rules.

5.2.5. Users who are supplied with computer equipment by OVP are responsible for the safety and care of that equipment, as well as the security of software and data stored it.

5.2.6. Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, users should take reasonable precautions to secure devices entrusted to their care.

5.2.7. Users must guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into OVP’s systems by whatever means and must report any actual or suspected malware infection to IT immediately.

5.2.8. Users are responsible to notifying IT and Legal of any unauthorized access or interception of electronic or physical records regardless of the encryption state.

5.3. Unacceptable Use

5.3.1. All employees should use their own judgment regarding what is unacceptable use of OVP systems. The activities below are provided as examples of unacceptable use; however, it is not exhaustive. Should an employee need to contravene these guidelines to perform their role, they should consult with, and obtain approval from their manager before proceeding.

5.3.1.1. All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services.

5.3.1.2. All activities detrimental to the success of the company, including sharing sensitive information outside the company.

5.3.1.3. All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business.

5.3.1.4. All activities that are inappropriate for OVP to be associated with and/or are detrimental to the company’s reputation.

6. Related Procedures

N/A

7. Appendix

N/A

8. Revision History

Revision #	Revision Date	Description of Changes	Author
00	05-Apr-2021	New Document	JOHN DOE