ЧЕК-ЛИСТ
БЕЗОПАСНОСТИ ЛИЧНОГО БРЕНДА

I. БЕЗОПАСНОСТЬ АККАУНТОВ

1. Доступ и авторизация

- Включена двухфакторная аутентификация (код по SMS/приложение/ключ).
- Отдельный рабочий номер и отдельная почта только для соцсетей.
- Пароли хранятся в менеджере паролей, не в заметках/браузере.
- Нет входа с личных/чужих устройств.

2. Управление доступом

- Точная ролевая модель: кто постит, кто согласовывает, кто редактирует.
- Доступ передаётся только через админ-панель, не через «сброс пароля».
- Регулярная проверка: кто имеет админ-права → удалить всех лишних.

II. СЛУЖЕБНАЯ БЕЗОПАСНОСТЬ

3. Информация на фото и видео - публикуем только если:

- нет документов на столе,
- нет экранов компьютеров,
- нет служебных схем, карт, графиков,
- нет людей, которых нельзя показывать.

4. Сроки и планы

Не публикуем:

- намёки на будущие решения, / незавершённые инициативы/ внутренние обсуждения, информацию, которая может повлиять на бизнес/рыночные решения.

5. Упоминание коллег и связей

- Не показывать рабочие переписки.
- Не выкладывать конфиденциальные встречи.
- Не светить «внутриведомственные» связи, если это может создать конфликты.

II. ЛИЧНАЯ БЕЗОПАСНОСТЬ

6. Геолокация

- Геотеги отключены.
- Публикация истории с локацией — только после ухода из места.
- Не показывать маршрут до дома/работы.

7. Семья и близкие

- Не публиковать фото детей, школы, дом, распорядок дня.
- Не показывать документы близких

- **8. Приватные данные**

Следить за тем, чтобы в кадр не попадали:

- номера автомобилей,
- пропуска,
- QR-коды,
- билеты, командировочные бумаги.

IV. РЕПУТАЦИОННАЯ БЕЗОПАСНОСТЬ

9. Тональность и формулировки

Перед публикацией спросить себя:

- Это не воспринимается как «официальная позиция» раньше времени?
- Нет ли двусмысленности?
- Не выглядит ли эмоционально, агрессивно, снисходительно?

I0. Правовые риски

Не публиковать:

- персональные данные,
- сведения следствия,
- конфиденциальную рабочую информацию,
- цитаты из документов без разрешения.

11. Антикризис

При скандалах:

- Ничего не постить «на эмоциях».
- Проверять факты.
- Писать только после согласования с пресс-службой.

V. ТЕХНИЧЕСКАЯ ГИГИЕНА

12. Устройства

- Телефон и ноутбук обновлены.
- Антивирус включён.
- Все мессенджеры защищены кодом/FaceID.

13. Wi-Fi

- Не входить в соцсети через общественные сети (кафе/аэропорт).
- В поездках использовать VPN (если это разрешено политикой ведомства).

14. Перемещения

В командировках избегать публикаций, которые показывают:

- схему безопасности мероприятия,
- расположение охраны,
- маршрут движения.

VI. КОМАНДНАЯ РАБОТА

15. Кто отвечает за что

- Чёткие правила: что публикуете лично ВЫ, что — команда.
- Таблица рисков: какие темы требуют обязательного согласования.
- Ведение «редакционного плана» (контент-плана) без сюрпризов.

ВШГУ